

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC945 U.S. PTO
09/705707
11/06/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2000年 2月 1日

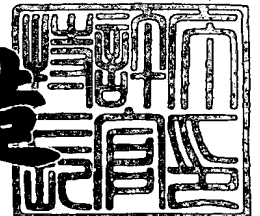
出願番号
Application Number: 特願2000-024519

出願人
Applicant(s): 富士ゼロックス株式会社

2000年 7月21日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3056421

【書類名】 特許願

【整理番号】 FE00-00023

【提出日】 平成12年 2月 1日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/00

【発明の名称】 予約証明証発行装置および方法

【請求項の数】 22

【発明者】

 【住所又は居所】 神奈川県足柄上郡中井町境4 3 0 グリーンテクなかい
 富士ゼロックス株式会社内

 【氏名】 京嶋 仁樹

【発明者】

 【住所又は居所】 神奈川県足柄上郡中井町境4 3 0 グリーンテクなかい
 富士ゼロックス株式会社内

 【氏名】 申 吉浩

【特許出願人】

 【識別番号】 000005496

 【氏名又は名称】 富士ゼロックス株式会社

 【電話番号】 0462-38-8516

【代理人】

 【識別番号】 100086531

 【弁理士】

 【氏名又は名称】 澤田 俊夫

 【電話番号】 03-5541-7577

【手数料の表示】

 【予納台帳番号】 038818

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 予約証明証発行装置および方法

【特許請求の範囲】

【請求項 1】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行する方法であって、

予約証明証の正当性を検証するために必要な検証用情報を作成するステップと

検証用情報を特定するための情報を入力するステップと、

入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な予約証明証を作成するステップと、

作成された予約証明証を出力するステップと

を備えていることを特徴とする予約証明証発行方法。

【請求項 2】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行するコンピュータシステムであって

予約証明証の正当性を検証するために必要な検証用情報を作成する検証用情報作成手段と、

上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、

検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な予約証明証を作成する予約証明証作成手段と、

上記予約証明証作成手段で作成された予約証明証を出力する予約証明証出力手段と

を備えることを特徴とする予約証明証発行システム。

【請求項 3】 予約内容を限定するための条件である予約条件を作成する予約条件作成手段を備え、

上記予約証明証作成手段が作成した予約証明証に、上記予約条件作成手段が作成した予約条件が含まれていることを特徴とする

請求項 2 記載の予約証明証発行システム。

【請求項 4】 上記予約証明証作成手段が、

検証用情報を特定するための情報とともに、予約証明証の依頼の仲介者を特定するための情報と、該特定される検証用情報に対応する予約証明証の依頼の仲介が該仲介者に許諾されていることを証明する予約証明証仲介許諾証が入力され、

予約証明証仲介許諾証によって該仲介者に該検証用情報に対応する予約証明証の依頼の仲介が許諾されているかを確認し、許諾されている場合にのみ予約証明証を作成することを特徴とする

請求項 2 記載の予約証明証発行システム。

【請求項 5】 予約証明証の発行履歴を記憶する予約証明証発行履歴記憶部と、

物品やサービスの提供者を特定するための情報の入力を受け、予約証明証発行履歴記憶部に記憶されている発行履歴から、該提供者が提供する物品やサービスに関する予約証明証の発行履歴である予約証明証提供者用発行履歴を抽出する予約証明証提供者用発行履歴作成部と、

前記予約証明証提供者用発行履歴作成部で作成された予約証明証提供者用発行履歴を出力する予約証明証提供者用発行履歴出力部とをさらに備えることを特徴とする

請求項 2 記載の予約証明証発行システム。

【請求項 6】 さらに、予約証明証の発行の依頼を受理する予約証明証発行依頼受理手段を備え、

上記予約証明証発行依頼受理手段が予約証明証発行依頼を受理した場合に、上記予約証明証作成手段で予約証明証を作成し、

予約証明証の発行履歴を記憶する予約証明証発行履歴記憶部と、

予約証明証発行の依頼者を特定するための情報の入力を受け、予約証明証発行履歴記憶部に記憶されている発行履歴から、該依頼者から依頼された予約証明証の発行履歴である予約証明証依頼者用発行履歴を抽出する予約証明証依頼者用発行履歴作成部と、

前記予約証明証依頼者用発行履歴作成部で作成された予約証明証依頼者用発行履歴を出力する予約証明証依頼者用発行履歴出力部とをさらに備えることを特徴

とする

請求項 2 記載の予約証明証発行システム。

【請求項 7】 検証用情報の発行履歴を記憶する検証用情報発行履歴記憶部と、

検証用情報の被発行者を特定するための情報の入力を受け、検証用情報発行履歴記憶部に記憶されている発行履歴から、該被発行者に対して発行された検証用情報に関する検証用情報の発行履歴である検証用情報発行被発行者用履歴を抽出する検証用情報発行履歴作成部と、

前記検証用情報発行履歴作成部で作成された検証用情報発行被発行者用履歴を出力する検証用情報発行履歴出力部とをさらに備えることを特徴とする

請求項 2 記載の予約証明証発行システム。

【請求項 8】 さらに、公開鍵暗号ペアを作成する公開鍵暗号ペア作成手段と、

上記公開鍵暗号ペア作成手段で作成された公開鍵ペアのうちの秘密鍵を保持する秘密鍵保持手段とを備え、

検証用情報が上記公開鍵暗号ペア作成手段で作成された公開鍵であり、

予約証明証が秘密鍵保持手段に保持されている秘密鍵を使用して作成されることを特徴とする

請求項 2 記載の予約証明証発行システム。

【請求項 9】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介する方法であって、

特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第 1 の予約証明証依頼を受領するステップと、

受領した第 1 の予約証明証依頼で依頼されている予約証明証の発行を依頼する第 2 の予約証明証依頼を作成するステップと、

作成された第 2 の予約証明証依頼を出力するステップと

を有することを特徴とする予約証明証仲介方法。

【請求項 10】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介するコンピュータシステム

であって、

特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第 1 の予約証明証依頼を受領する予約証明証依頼受領手段と、

受領した第 1 の予約証明証依頼で依頼されている予約証明証の発行を依頼する第 2 の予約証明証依頼を作成する予約証明証依頼作成手段と、

上記予約証明証依頼作成手段で生成された第 2 の予約証明証依頼を出力する予約証明証依頼出力手段と

を有することを特徴とする予約証明証仲介システム。

【請求項 1 1】 特定の予約証明証の正当性を検証するために必要な検証用情報が特定の物品やサービスに対応づけられており、

第 1 および第 2 の予約証明証依頼に、該依頼が予約証明証を依頼する物品やサービスを特定するために検証用情報を特定するための情報が含まれる

ことを特徴とする請求項 1 0 記載の予約証明証仲介システム。

【請求項 1 2】 依頼する予約証明証が予約内容を限定するための条件である予約条件を含むものであり、

依頼する予約証明証に含まれるべき予約条件を作成する予約条件作成手段を備え、

予約証明証依頼作成手段が作成した第 2 の予約証明証依頼に、上記予約条件作成手段が作成した予約条件が含まれることを特徴とする

請求項 1 0 記載の予約証明証仲介システム。

【請求項 1 3】 自らが特定の物品やサービスに対する予約証明証の依頼の仲介を許諾されていることを証明する予約証明証仲介許諾証を保持する予約証明証仲介許諾証記憶手段を備え、

予約証明証依頼出力手段が作成する予約証明証依頼に、予約の対象となる物品やサービスに対するものであり、かつ、予約証明証仲介許諾証記憶手段に保持されている予約証明証仲介許諾証を添付することを特徴とする

請求項 1 0 記載の予約証明証仲介システム。

【請求項 1 4】 さらに、第 1 の予約証明証依頼の依頼者に予約証明証発行料金の課金を行う課金手段を備え、

第1の予約証明証依頼が入力された時に、上記課金手段によって所定の予約証明証発行料金を該依頼者に対して課金することを特徴とする

請求項10記載の予約証明証仲介システム。

【請求項15】 さらに、第1の予約証明証依頼の依頼者から予約証明証発行料金を徴収する決済手段を備え、

第1の予約証明証依頼が入力された時に、上記決済手段によって所定の予約証明証発行料金を該依頼者から徴収することを特徴とする

請求項10記載の予約証明証仲介システム。

【請求項16】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾する方法であって、

物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報を入力するステップと、

該仲介者に仲介を許諾する物品やサービスを特定するための情報を入力するステップと、

入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成するステップと、

作成された予約証明証仲介許諾証を出力するステップとを有することを特徴とする予約証明証仲介許諾方法。

【請求項17】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾するコンピュータシステムであって、

物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾する物品やサービスを特定するための情報とが入力され、入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成する予約証明証仲介許諾証作成手段と、

上記予約証明証仲介許諾証作成手段で作成された予約証明証仲介許諾証を出力する予約証明証仲介許諾証出力手段と

を有することを特徴とする予約証明証仲介許諾システム。

【請求項 18】 許諾証の受け手である仲介者が仲介することで発行される予約証明証に記載される予約内容を限定するための条件である予約条件の範囲を限定するための情報である予約条件限定情報を作成する予約条件限定情報作成手段を備え、

上記予約証明証仲介許諾証作成手段が作成した予約証明証仲介許諾に、上記予約条件限定情報作成手段が作成した予約条件限定情報が含まれていることを特徴とする

請求項 17 記載の予約証明証仲介許諾システム。

【請求項 19】 許諾証の発行履歴を記憶する予約証明証仲介許諾証発行履歴記憶部と、

予約証明証の依頼の仲介者を特定するための情報の入力を受け、予約証明証仲介許諾証発行履歴記憶部に記録されている発行履歴から、該仲介者に対して発行された許諾証に関する履歴である予約証明証仲介許諾証発行仲介者用履歴を抽出する予約証明証仲介許諾証発行仲介者用履歴作成部と、

前記予約証明証仲介許諾証発行仲介者用履歴作成部で作成された予約証明証仲介許諾証発行仲介者用履歴を出力する予約証明証仲介許諾証発行仲介者用履歴出力部とをさらに備えることを特徴とする

請求項 17 記載の予約証明証仲介許諾システム。

【請求項 20】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する方法であって、

予約証明証を検証するための検証用情報を記憶するステップと、

予約証明証を入力するステップと、

入力された予約証明証の正当性を記憶した検証用情報を使用して検証するステップと

を有することを特徴とする予約証明証検証方法。

【請求項 21】 物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する装置であって、

予約証明証を検証するための検証用情報を記憶する検証用情報記憶手段と、

予約証明証が入力され、その予約証明証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する予約証明証検証手段とを有することを特徴とする予約証明証検証装置。

【請求項 2 2】 さらに、予約証明証を保持している携帯用記憶装置を接続する接続手段を備え、

予約証明証検証手段が、上記接続手段を通して接続された携帯用記憶装置に記憶されている予約証明証の正当性を検証することを特徴とする請求項 2 1 記載の予約証明証検証装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、コンピュータシステムにおいて物品あるいはサービスを予約する技術に関わり、特に、消費者が物品あるいはサービスを予約していることを証する予約証明証の発行や、該予約証明証の正当性の検証に関する。

【0 0 0 2】

【従来の技術】

特定の場所や特定の時間に限られることの多い物品の取得あるいはサービスの提供を、取得や提供の場所や時間とは独立に許諾する方法として現在もっとも広範に使用されているのは、予約証明証の配布である。

【0 0 0 3】

購入希望者が殺到しそうな物品に対して、発売以前に予約を受けつけ、発売時には予約を行った消費者に優先的に物品を発売するという物品の販売方法は非常に広範に行われている。予約済の消費者とそうでない消費者とを区別するために、予約したことを証するものが配布される。この予約証明証は、種々の情報が印刷された紙であったり、あるいは番号であったりする。対価の支払いが物品の引き渡し時に行われる場合もあるし、予約時に行われる場合もある。

【0 0 0 4】

サービスの提供では、プレイガイド等のチケット販売業者の窓口で事前に販売される映画やコンサート等の前売り券が最も典型的な例である。この場合には、

情報が紙に印刷されたチケットが予約証明証である。

【0005】

消費者の家庭にコンピュータが普及し、多くの消費者が日常的にインターネットに接続するようになった昨今では、インターネット上に構築されたサイトで様々な予約が可能になってきた。サイトで予約を依頼したユーザに対して予約証明証にあたるデジタルデータを発行し、物品やサービスの提供時に消費者から発行したデータの提示を受け、予約証明証が正当なものであれば物品やサービスを提供するといったものが典型的な取り引きの方法である。

【0006】

インターネットを利用した物品やサービスの予約販売は、消費者にとっては、家庭にいながら様々な物品やサービスの予約が可能であるというメリットをもたらした。また、物品やサービスの販売者にとっては物理的な店舗を維持するコストを払うことなく販売経路を拡大できるという利点があり、特に広範な販売店舗網を維持できない小規模な業者にとって、なくてはならない販売経路となりつつある。

【0007】

【発明が解決しようとする課題】

現在のインターネットを利用した物品やサービスの予約販売は、予約販売業者毎に独立に行われている。各予約販売業者は独自のサイトを運営し、そのサイトで独自の予約証明証を生成し消費者に発行する。各業者は、予約証明証を発行するために必要な開発をそれぞれ独自に行わなければならない上に、予約証明証を発行するサイトの運営コストもそれぞれが負担しなければならない。偽造や複製という危険性を持つ予約証明証というデジタルデータを扱うシステムを運営することは深刻なコストの上昇をもたらし、予約販売業者がインターネットでの予約販売に乗り出す際の重大な障壁になるとともに、販売価格の上昇という不利益を消費者にもたらす。

【0008】

【課題を解決するための手段】

本発明では、予約販売される特定の物品やサービスあるいは特定の予約販売業

者とは独立の予約証明証の発行を担うサーバ（以降、予約証明証発行センタあるいは単にセンタとよぶ）をインターネット上に構築することで、上記の課題を解決する。予約証明証の作成や維持に関わる部分は予約証明証発行センタがすべて引き受け、物品やサービスの予約販売を行う業者は予約証明証に関わる部分の多くを予約証明証発行センタにアウトソーシングすることができる。多くの予約販売業者が共通の予約証明証発行センタを使用することが可能なので、予約販売業者一つあたりの予約証明証発行センタの開発・運営コストは予約販売業者が独自の予約販売システムを構築するのにくらべて低く押さえることができる。

【0009】

本発明では、各予約販売業者は、消費者から受けた予約依頼に対して予約証明証を発行するが、その予約証明証は予約証明証発行センタで生成される。予約販売業者は、消費者からの予約の依頼を受け付けるサーバをインターネット上に構築するが、予約証を生成する部分は該サーバ中には存在せず、予約証明証発行センタがその役割を担う。

【0010】

物品やサービスの提供時には、消費者から予約証明証の提示を受け、予約証明証の正当性が検証されるが、この検証は検証用情報と呼ばれるデジタルデータを使用して行われる。検証用情報は複数の予約証明証との間に所定の関係を満たすように生成されており、検証用情報と予約証明証がその関係を満たすかどうかで予約証明証の正当性が判定される。特定の物品やサービスと特定の検証用情報をバインドさせておけば、その検証用情報と所定の関係を満たす予約証明証を提示できるかどうかで、消費者が正しく予約をしたかどうか判定できる。

【0011】

検証用情報は、センタで生成され出力される。どの予約販売業者が販売した予約証明証であっても検証用情報を入手していればその正当性を検証することが可能である。

【0012】

この特徴は、物品やサービスの予約販売ビジネスをに乗り出す業者が払うべきコストを更に下げる効果を持つ。本発明では、物品やサービスの提供者と、それ

らの予約販売の業者は互いに独立に存立できる。物品やサービスの提供者は、自分が提供する物品やサービスの予約販売を多くの予約販売業者に委託し、自己は物品やサービスの提供に専念することができる。また、予約販売業者は、自らが提供する物品やサービスをまったく持たなくても、様々な提供者が提供する多くの物品やサービスを予約販売する事が可能である。

【0013】

請求項1または2に記載の発明は予約発行センタに関するものである。

【0014】

請求項1に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行する方法であって、予約証明証の正当性を検証するために必要な検証用情報を作成するステップと、検証用情報を特定するための情報を入力するステップと、入力された検証用情報を特定するための情報によって特定される検証用情報で検証可能な予約証明証を作成するステップと、作成された予約証明証を出力するステップとを備える。

【0015】

また、請求項2に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証を発行するコンピュータシステムであって、予約証明証の正当性を検証するために必要な検証用情報を作成する検証用情報作成手段と、上記検証用情報作成手段で作成された検証用情報を出力する検証用情報出力手段と、検証用情報を特定するための情報が入力され、該入力によって特定される検証用情報で検証可能な予約証明証を作成する予約証明証作成手段と、上記予約証明証作成手段で作成された予約証明証を出力する予約証明証出力手段とを備える。

【0016】

請求項1または2に記載の発明による予約発行センタは、予約証明証を発行するだけでなく、予約証明証を検証するための検証用情報も出力する。この検証用情報は物品やサービスの提供の際に消費者から提示される予約証明証の正当性を検証する際に使用される。特定の検証用情報によって検証可能な予約証明証の集合は限定されるので、特定の物品やサービスに検証用情報を割り当てることで、

物品毎あるいはサービス毎の予約証明証の発行が可能である。しかし、どの検証用情報（あるいはそれに対応する予約証明証の集合）がどの物品やサービスに対応するかに関して予約発行センタは関与する必要はない。特定の物品やサービスと検証用情報との連結は物品やサービスの提供者が自由に決定することができる。このことが、予約証明証発行センタを、特定の物品やサービスに関与しない予約証明証の発行にのみ特化したインフラストラクチャたらしめることを可能にする。

【 0 0 1 7 】

請求項 9 または 1 0 に記載の発明は、物品やサービスの予約販売を行うサーバに関するものである。

【 0 0 1 8 】

請求項 9 に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介する方法であって、特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第 1 の予約証明証依頼を受領するステップと、受領した第 1 の予約証明証依頼で依頼されている予約証明証の発行を依頼する第 2 の予約証明証依頼を作成するステップと、作成された第 2 の予約証明証依頼を出力するステップとを有することを特徴とする。

【 0 0 1 9 】

また、請求項 1 0 に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼を仲介するコンピュータシステムであって、特定の物品やサービスの提供の予約を証する予約証明証の発行の依頼である第 1 の予約証明証依頼を受領する予約証明証依頼受領手段と、受領した第 1 の予約証明証依頼で依頼されている予約証明証の発行を依頼する第 2 の予約証明証依頼を作成する予約証明証依頼作成手段と、上記予約証明証依頼作成手段で生成された第 2 の予約証明証依頼を出力する予約証明証依頼出力手段とを有することを特徴とする。

【 0 0 2 0 】

請求項 9 または 1 0 に記載の発明を適用した、物品やサービスの予約販売を行

うサーバは、インターネットに接続している消費者あるいは他の予約販売業者からの予約証明証発行の依頼を受けつける。しかし、受け付けた依頼に対する予約証明証を作成するのはこのサーバではない。予約証明証の発行は予約証明証発行センタのみが行い、物品やサービスの予約販売を行うサーバは、予約証明証発行の仲介のみを行う。該サーバが行うのは、単に依頼の仲介のみであり、予約証明証の改竄、偽造、複製といった攻撃に対する配慮はセンタが行うので、本実施例に基づいた物品やサービスの予約販売を行うサーバの構築費用や運営コストは低く押さえられる。

【0021】

請求項16または17に記載の発明は、物品やサービスの提供者に関するものである。

【0022】

物品やサービスの提供者と予約販売業者が独立に存立した場合、該提供者にとっては、自己が提供する物品やサービスをより多くの予約販売業者に予約販売をしてもらうほうが、基本的には有利である。しかし、信頼できない予約販売業者に自己の物品やサービスを扱われることは、後のトラブルを招く恐れが高く許容できない。したがって、物品やサービスの提供者が、自己の物品やサービスを扱える予約販売業者を限定できる手段が必要になる。

【0023】

請求項16に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾する方法であって、物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報を入力するステップと、該仲介者に仲介を許諾する物品やサービスを特定するための情報を入力するステップと、入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成するステップと、作成された予約証明証仲介許諾証を出力するステップとを有することを特徴とする。

【0024】

また、請求項17に記載の発明は、物品やサービスの提供が特定の消費者に対

して予約されていることを証明する電子的な予約証明証の依頼の仲介を許諾するコンピュータシステムであって、物品やサービスの予約証明証の依頼を仲介する仲介者を特定するための情報と、該仲介者に仲介を許諾する物品やサービスを特定するための情報とが入力され、入力によって特定された物品やサービスに対する予約証明証の依頼の仲介が入力によって特定された仲介者に許諾されていることを証明する予約証明証仲介許諾証を作成する予約証明証仲介許諾証作成手段と、上記予約証明証仲介許諾証作成手段で作成された予約証明証仲介許諾証を出力する予約証明証仲介許諾証出力手段とを有することを特徴とする。

【 0 0 2 5 】

請求項 1 6 または 1 7 に記載の発明によれば、物品やサービスの提供者は、自己が提供する物品やサービスの予約販売を許す予約販売業者に対して予約証明証仲介許諾証を発行する。この予約証明証仲介許諾証は、予約販売業者が予約証明証の発行をセンタに依頼する場合にセンタに対して提示される。センタは提示された予約証明証仲介許諾証により、該予約販売業者が予約証明証の発行を依頼した物品やサービスに対する予約販売を許諾されているかどうかを検査することができる。

【 0 0 2 6 】

請求項 2 0 または 2 1 に記載された発明は、予約証明証の検証に関するものである。

【 0 0 2 7 】

請求項 2 0 に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する方法であって、予約証明証を検証するための検証用情報を記憶するステップと、予約証明証を入力するステップと、入力された予約証明証の正当性を、記憶した検証用情報を使用して検証するステップとを有することを特徴とする。

【 0 0 2 8 】

また、請求項 2 1 に記載の発明は、物品やサービスの提供が特定の消費者に対して予約されていることを証明する電子的な予約証明証の正当性を検証する装置であって、予約証明証を検証するための検証用情報を記憶する検証用情報記憶手

段と、予約証明証が入力され、その予約証明証の正当性を前記検証用情報記憶手段に記憶されている検証用情報を使用して検証する予約証明証検証手段とを有することを特徴とする。

【0029】

なお、本発明は予約証明証を発行するためにインフラストラクチャを予約販売業者と独立に提供することを可能とするものであるが、副次的に、予約販売業者や、商品やサービスの提供者と関連する証明証発行センタが、本発明を利用して予約証明証を発行するようにしてもよいことはもちろんである。また、商品やサービスの提供者が予約販売を直接に行う場合にも本発明の予約証明証発行センタを利用できる。

【0030】

また、証明証の発行はインターネット以外の通信手段例えば電話回線を利用して行うようにしてもよい。また携帯記録媒体等を用いて機器の間で証明証のやり取りを行うようにしてもよい。

【0031】

なお、予約は将来商品やサービスの提供を受けたい旨の意思表示であり、商品やサービスを購入してその提供を将来受けるものであればよく、発売日以前の予約のみに限定されない。例えば、ある時点で商品購入の申込を行なうとともに決済を済ませ、数日後にその商品を自宅やコンビニエンスストア等で受け取るというものでよい。この場合には、申込の証明証あるいは決済済みの証明証ということもできる。ここでは同じ意味である。

【0032】

また、履行期が異なる双務的な取引あるいは契約があるときに、一方の債務、例えば金銭の支払が履行されたときにこれを証明する証明証を発行し、反対債務の受給を受けるときにこの証明証で先行債務の履行を証明する場合に、この発明を広く適用できる。

【0033】

【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

【 0 0 3 4 】

図 1 は本発明を適用した実施例の構成図である。本実施例は、インターネットに接続した複数のコンピュータシステムからなり、これらが協調して動作することで物品やサービスの予約販売を行う。

【 0 0 3 5 】

本実施例では、消費者は物品やサービスの予約をインターネット経由で行い、予約が完了したことを証するデジタルデータである予約証明証を受け取る。ユーザは受け取った予約証明証を IC カード等の携帯型記憶装置に記憶した後、物品やサービスの提供を受ける場所に携行する。消費者が物品やサービスの提供を受ける場所には、予約証明証の検証を行う携帯型記憶装置を接続可能な検証用機器が設置されており、この機器によって予約証明証の正当性が検証されれば、消費者に物品やサービスが提供される。

【 0 0 3 6 】

〔実施例を構成するコンピュータシステム群〕

本実施例を構成するコンピュータシステムは以下の 4 つの種類に分類される。それぞれインターネット 1 0 1 に接続され、相互に通信を行う。

【 0 0 3 7 】

消費者端末：消費者が物品やサービスの予約を行う際に使用するコンピュータシステム。図 1 の 1 0 9 にあたる。消費者が家庭で使用するコンピュータであってもよいし、コンビニエンスストアに設置されている端末でもよい。インターネット 1 0 1 に接続されており、インターネット 1 0 1 経由で他のコンピュータシステムにアクセスすることができる。

【 0 0 3 8 】

消費者端末 1 0 9 は IC カード等の携帯型記憶装置を接続することが可能であり、消費者が持つ携帯型記憶装置 1 1 0 が接続され、消費者が取得した予約証明証が携帯型記憶装置 1 1 0 に記録される。また、消費者端末と携帯型記憶装置の機能を兼ねるものとして、ノート型のコンピュータや携帯電話を利用してもよい。

【 0 0 3 9 】

図 1 では、単一の消費者端末のみ図示しているが、インターネットに接続される同様の無数のコンピュータが消費者端末として使用される。

【 0 0 4 0 】

消費者端末を使用する消費者が保持する携帯型記憶装置には、消費者を特定するための識別子である消費者識別子と、消費者自身もその値を知る事ができない秘密情報である消費者秘密情報が格納されている。

【 0 0 4 1 】

消費者識別子と消費者秘密情報のペアはセンタによって保持されており、予約証明証の生成に利用される。

【 0 0 4 2 】

リテーラ：消費者に対して物品やサービスの予約販売を行うコンピュータシステム。図 1 の 1 0 3 あるいは 1 0 4 にあたり、実際にはいくつ存在してもかまわない。インターネット 1 0 1 に接続されており、インターネット 1 0 1 経由で消費者からのアクセスを受け付ける。リテーラを運営しているのは物品やサービスの予約販売をしている業者であるが、以降の本実施例の説明では、該コンピュータシステムと該業者を区別せず、ともにリテーラと呼ぶ事にする。

【 0 0 4 3 】

予約証明証発行センタ：予約証明証を生成し発行するコンピュータシステム。図 1 の 1 0 2 にあたる。インターネット 1 0 1 に接続されており、インターネット経由で予約証明証の依頼を受け付け、オンデマンドで予約証明証を作成し発行する。以降、センタといえは予約証明証発行センタを指す。

【 0 0 4 4 】

プロバイダ：物品やサービスの提供者がリテーラ 1 0 3 あるいは 1 0 4 やセンタ 1 0 2 と情報の交換を行うためのコンピュータシステムであり、インターネット 1 0 1 に接続される。図 1 の 1 0 5、1 0 7 にあたり、実際にはいくつ存在してもかまわない。以降の本実施例の説明では、物品やサービスの提供者と該提供者が使用するコンピュータシステムを区別せず、ともにプロバイダと呼ぶ事にする。

【 0 0 4 5 】

認証局 (Certificate Authority: CA) : 消費者端末、リテラ、センタ、プロバイダのあいだで交わされる各メッセージには、改竄検知と否認拒否のためにデジタル署名が施される。そのデジタル署名の公開鍵の正当性は X. 509 ベースの公開鍵証明書によって保証される。Certificate Authority 111 はこの公開鍵証明書を作成し発行する機能を持つコンピュータシステムであり、インターネット 101 に接続されている。また、Certificate Authority は、自己が発行した公開鍵証明書を保持しており、オンデマンドで要求者に送付する機能も持つ。以降、CA といえば Certificate Authority を指す。

【0046】

[予約証明書と検証用公開鍵]

本実施例では、消費者が物品やサービスを予約したことを証明するために予約証明書と呼ばれるデジタルデータが発行される。予約証明書の正当性は対応する検証用公開鍵によって検証される。検証用公開鍵の名前が示すように、本実施例では予約証明書と検証用公開鍵には公開鍵暗号技術が応用される。

【0047】

より具体的には、検証用公開鍵は公開鍵暗号における公開鍵であり、予約証明書は該公開鍵に対応する秘密鍵をもとに作成された予約値を含むデータである。予約証明書が含む予約値を作成する際に使用した秘密鍵と、検証用公開鍵が対応するものであった場合にのみ、予約証明書が正当なものであることが確認でき、それ以外の場合で予約証明書が正当なものであると認められることはない。

【0048】

本実施例で物品やサービスを予約販売する場合には、予約販売される特定の物品やサービスとバインドされる検証用公開鍵が必要である。特定の検証用公開鍵と特定の物品やサービスをバインドさせることで、特定の物品やサービスにのみ有効な予約証明書を実現することができる。

【0049】

予約証明書と検証用公開鍵に公開鍵暗号技術を利用しているのは、検証用公開鍵を公開可能とするためである。検証用公開鍵が公開鍵であれば、それを公開し

ても予約証明証の安全性を損なうことがない。このことは、検証用公開鍵の送受信や管理を楽にするだけでなく、予約証明証の正当性を第三者が検証できるようになり、後のトラブルを防ぐことが可能になるという利点がある。

【0050】

検証用公開鍵はプロバイダからの依頼によって、センタ102で作成され、検証用公開鍵情報と呼ばれるデータに含まれて依頼者に送付される。センタ102は、検証用公開鍵の発行の要求を受け取ると新しい公開鍵ペアを作成し、その公開鍵と秘密鍵を公開鍵ペアを一意に識別するための情報である検証用公開鍵識別子とともに保持した後、その公開鍵と検証用公開鍵識別子を含む検証用公開鍵情報を依頼者に送付する。検証用公開鍵情報を受け取ったプロバイダを、その検証用公開鍵情報あるいは該検証用公開鍵情報に含まれる検証用公開鍵のユーザと呼ぶ。

【0051】

特定の検証用公開鍵と特定の物品やサービスのバインドに関してセンタ102は関知しない。そのバインドを決定するのは、検証用公開鍵の発行を受けたプロバイダであり、該プロバイダは、自分が決定した特定の物品やサービスと検証用公開鍵とのバインドの情報を保持しておかなければならない。

【0052】

検証用公開鍵の発行を受けたプロバイダは、該検証用公開鍵に対応する物品やサービスの予約証明証を、検証する機器106、108に設定する。

【0053】

消費者はインターネット上でリテラを介して特定の物品やサービスに対する予約証明証を取得する。取得した予約証明証は、消費者が持つ携帯型記憶装置に記憶される。消費者は物品を入手したりサービスの提供を受けたりする場所に該携帯型記憶装置を持参し、そこにある検証機器106、108に携帯型記憶装置を接続して予約証明証の正当性の検証を受ける。

【0054】

物品の予約販売の場合には、物品の引き渡し窓口に予約証明証の検証機器を設置しておき、その検証機器で予約証明証の正当性を検証された消費者のみに物品

を提供する。物品の引き渡し場所は、コンビニエンス・ストアや駅の売店等、検証機器が設置可能な場所であればどこでもよい。

【 0 0 5 5 】

これらの実施形態で消費者に提供される物品は、コンサートや映画の入場券、列車や旅客機への搭乗券、ホテル等の宿泊券等の紙製のチケットの類も含まれる。この場合、コンサートや映画の入場窓口やチケット販売店の窓口、駅や空港の窓口あるいは旅行代理店等に予約証明証の検証機器を設置しておき、そこで予約証明証の正当性を検証した後で引き渡すという実施形態が取れる。

【 0 0 5 6 】

また、検証機器と物品の提供を自動的に連動させた一台の筐体にして、予約証明証の検証後に、自動的に物品が搬出される、自動販売機のような実施形態も取り得る。

【 0 0 5 7 】

また、予約された物品を配達する場合には、配達者が予約証明証を検証する携帯機器を持参し、配達先で物品を引き渡す前に、消費者が所持する予約証明証の正当性を検証し、検証に成功した場合にのみ物品を引き渡すといった方法も可能である。

【 0 0 5 8 】

コンサートや映画の入場といったサービスの提供の場合には、コンサート会場の入場ゲートに予約証明証の検証機能を実装しておき、消費者が入場する際に消費者が持参した予約証明証の正当性を検証して、検証に成功した場合にのみ入場を許すといった実施形態も考えられる。

【 0 0 5 9 】

また、コンサート会場や映画館の特定の座席の使用が提供されるサービスである場合には、該座席に予約証明証の検証機器を付属させ、その座席の検証機器で予約証明証の正当性の検証に成功した消費者のみがこの座席に座ることが許されるように構成すればよい。列車や航空機への入場あるいはその特定の座席の使用といったサービスにおいても同様の方法が利用可能である。

【 0 0 6 0 】

コンサートや映画、列車や航空機の入場あるいは座席指定においては、係員が携帯型の検証器を所持して、各座席を回って座席の使用者が正しい予約証明証を保持することを検証するという実施形態も好適である。

【0061】

ホテルの部屋の使用というサービスを提供する場合には、ホテルのフロントに検証用機器を置き、それによって予約証明証の正当性を検証する。また、検証用機器を部屋の鍵と連動するように設置し、消費者が持参した予約証明証の検証に成功した場合のみ開錠されるように実装すれば、フロントでの処理を軽減できて効果的である。ロッカー、倉庫等の使用においても同様の実施形態をとることができる。

【0062】

物品といっても、物理的なものではなく、デジタルデータ等であってもよい。たとえば、インターネット上にある楽曲や画像およびソフトウェア等のデジタルデータのダウンロードの予約に適用することもできる。この場合、検証機器はインターネット上にあるサイトとして実現し、消費者は、家庭にあるPCあるいはコンビニ等に設置されている端末から、インターネットを介して検証を行うサイトに予約証明証を提示する。該サイトは、提示された予約証明証の正当性の検証に成功した場合にのみ、消費者にデータのダウンロードを許す。

【0063】

予約証明証を記憶する携帯型記憶装置としては、記憶機能のみを持つメモリカードやICカード、あるいは計算機能も持つスマートカードなどが利用可能である。接触型あるいは非接触型のどちらでもよい。特に混雑が予想されるコンサート等の入場ゲートに検証用機器を設置する場合には、非接触型のものが望ましい。

【0064】

携帯電話のように、インターネットに接続可能な端末であってしかも携帯可能なものも好ましい実装の形態である。特に無線での通信機能を持つ携帯型の機器を利用するのは、消費者の利便性も向上し、好適である。

【0065】

検証用公開鍵情報のデータ構造は以下のようである。

【 0 0 6 6 】

【表 1】

検証用公開鍵情報：：＝ {

発行者フィールド，
受領者フィールド，
発行日フィールド，
有効期間開始日時フィールド，
有効期間終了日時フィールド，
検証用公開鍵識別子フィールド，
公開鍵情報フィールド，
デジタル署名フィールド

}

【 0 0 6 7 】

発行者フィールド：この検証用公開鍵情報の発行者であるセンタの識別子が記載される。

受領者フィールド：この検証用公開鍵情報の受領者であるプロバイダの識別子が記載される。

発行日フィールド：この検証用公開鍵情報の発行日が記載される。

有効期間開始日時フィールド：この検証用公開鍵情報の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この検証用公開鍵情報の有効期間の終了日時が記載される。

検証用公開鍵識別子フィールド：センタがこの検証用公開鍵に割り当てた検証用公開鍵識別子が記載される。

公開鍵情報：予約証明証を検証する際に使用する公開鍵の情報が記載される。使用する公開鍵暗号アルゴリズムの指定と、公開鍵の値を含む。

デジタル署名フィールド：発行者であるセンタによるこの検証用公開鍵情報全体に対するデジタル署名が記載される。

【0068】

予約証明証のデータ構造は以下のようである。

【0069】

【表 2】

予約証明証 ::= {

発行者フィールド,
受領者フィールド,
発行日フィールド,
予約証明証識別子フィールド,
公開鍵識別子フィールド,
予約条件フィールド,
予約値フィールド,
デジタル署名フィールド

}

【0070】

発行者フィールド：この予約証明証の発行者であるセンタの識別子が記載される。

受領者フィールド：この予約証明証の受領者である消費者の識別子が記載される。

発行日フィールド：この予約証明証の発行日が記載される。

予約証明証識別子フィールド：センタがこの予約証明証に割り当てた識別子が記載される。

公開鍵識別子フィールド：この予約証明証に対応する検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

予約条件フィールド：この予約が有効である範囲を限定する条件である予約条件が記載される。

予約値フィールド：この予約証明証の公開鍵識別子フィールドに記載された識別子が割り当てられた検証用公開鍵に対応する秘密鍵をもとに作成されたデータが記載される。

デジタル署名フィールド：発行者であるセンタによるこの予約証明証全体に対するデジタル署名が記載される。

【0071】

予約条件には、この予約証明証での予約の有効な範囲を限定するための条件が記載される。

【0072】

予約条件のデータ構造を以下に示す。

【0073】

【表3】

予約条件 ::= {
 有効期間開始日時フィールド,
 有効期間終了日時フィールド,
 ...
 }

【0074】

有効期間開始日時フィールド：この予約証明証の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この予約証明証の有効期間の終了日時が記載される。

【0075】

予約条件に指定された各種条件は、予約証明証の検証時に該条件が満足されているかどうかを検査される。予約条件に指定された各種条件が満足されていなければ、予約証明証の正当性の検証に失敗する。

【0076】

予約条件には、有効期間の開始日時または終了日時以外にも、予約証明証の用途に応じて種々のものが記載される。

【0077】

たとえば、その予約証明証がコンサートやイベントの会場あるいは列車や旅客機の特定の座席を予約するものであった場合、その座席番号を予約条件に指定す

れば、該予約条件を含む予約証明証がその座席のみを予約したものであることが証明される。特定のイベントあるいは特定の列車や旅客機のみを予約する場合には、そのイベント名や車番、機番を予約条件に指定すればよい。特定の日時のイベントや搭乗に対する予約であれば、その日付を予約条件に指定する。

【0078】

また、特定の品名や品番を持つ物品に対する予約であった場合には、その品名や品番を予約条件に指定すればよい。

【0079】

さらに、物品やサービスの提供時に提供窓口で消費者から料金を徴収する場合、その料金の額を予約条件に指定し、その料金の額が物品やサービスの提供窓口で支払われた場合にのみ、予約証明証の検証に成功するよう構成することもできる。同様に、値引き額を予約条件に指定したり、物品やサービスの提供時にマイレージ等のポイントを消費者に与える場合には、与えるポイントの高を予約条件に指定することもできる。

【0080】

また、予約証明証の検証を行う機器や検査者を特定する情報を予約条件に指定し、指定された機器や検査者のみが予約証明証の検証に成功するように構成することもできる。

【0081】

[予約値]

予約値は予約証明証に含まれるデータである。センタが作成した検証用公開鍵に対応する秘密鍵を元に作成されたデータであり、予約証明証が特定の検証用公開鍵とのみ対応する事を保証するためのものである。また、予約値の作成には、各消費者が持つ秘密情報である消費者秘密情報や、予約証明証に記載された予約条件も使用され、特定の消費者のみが利用可能である事や、特定の予約条件を満足する場合にのみ利用可能である事も保証される。

【0082】

予約値 t は法数 n 、検証用公開鍵 e 、秘密鍵 d 、消費者秘密情報 u 、予約条件 l から以下の式にしたがって作成される。

【0083】

【数1】

$$t = d - f(n, e, u, l) \quad (1)$$

ここで、関数 $f()$ は公開された一方向性関数である。たとえば、SHA-1 あるいはMD5等の暗号学的一方向性ハッシュ関数が使用される。

【0084】

式(1)でわかるように、予約値 t は、法数 n 、検証用公開鍵 e 、消費者秘密情報 u 、予約条件 l とともに使用した場合にのみ秘密鍵 d と同じ働きをする。どれ一つを差し替えても秘密鍵 d と同じ働きをすることはない。

【0085】

[予約証明証の検証]

予約証明証の検証は、予約値 t が秘密鍵 d と同じ働きができるかどうかを判定する処理である。検証の方法には、いくつかのバリエーションが考えられる。

【0086】

図28は、消費者が保持する携帯型記憶装置が演算機能を持っている場合の、該携帯型記憶装置と予約証明証の検証機器の構成例を示した図である。携帯型記憶装置が、スマートカードや携帯電話、あるいはノートPCで実現される場合がこれにあたる。

【0087】

図28において、2801は予約証明証検証機器、2811は予約証明証検証機器2801に接続される携帯型記憶装置である。予約証明証検証機器2801は、チャレンジと呼ぶ乱数値を携帯型記憶装置2811に送付し、携帯型記憶装置2811は受け取ったチャレンジと保持している予約証明証からレスポンスと呼ぶ値を計算して出力し、予約証明証検証機器2801がレスポンスの正しさを検査する事で、携帯型記憶装置2811に保持されている予約証明証の正当性を検証する。

【0088】

予約証明証検証機器2801は、条件指定記憶部2802、チャレンジ生成部2803、公開鍵情報記憶部2804、レスポンス検査部2805、携帯型記憶

装置制御部 2806 から構成される。

【0089】

予約証明証検証機器 2801 の各部の役割を以下に示す。

【0090】

条件指定記憶部 2802 : 予約証明証検証機器 2801 が、予約証明証に記載されている予約条件が特定の条件を満たす場合にのみ予約証明証の検証に成功するよう構成する場合、予約条件に関する指定が保持される。

チャレンジ生成部 2803 : 携帯型記憶装置 2811 に送付するチャレンジを生成する。

公開鍵情報記憶部 2804 : この予約証明証検証機器に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

レスポンス検査部 2805 : 携帯型記憶装置 2811 が作成したレスポンスの正しさを検査する。

携帯型記憶装置制御部 2806 : 携帯型記憶装置 2811 との間の情報のやり取りを制御する。

【0091】

また、携帯型記憶装置 2811 は入出力制御部 2812、消費者秘密情報記憶部 2813、レスポンス計算部 2814、予約条件判定部 2815、予約証明証記憶部 2816 から構成される。

【0092】

携帯型記憶装置 2811 の各部の役割を以下に示す。

【0093】

入出力制御部 2812 : 予約証明証検証機器 2801 との間のデータの入出力を制御する。

消費者秘密情報記憶部 2813 : 消費者秘密情報を保持する。

レスポンス計算部 2814 : 予約証明証検証機器 2801 に送付するレスポンスを計算する。

予約条件判定部 2815 : 予約証明証に記載されている予約条件が満たされているかどうかを判定する。

予約証明証記憶部 2816：予約証明証が複数保持される。

【0094】

図 29 は、予約証明証の検証の際の予約証明証検証機器 2801 と携帯型記憶装置 2811 の動作を示すフローチャートである。図 29 に従って予約証明証の検証の際の予約証明証検証機器 2801 と携帯型記憶装置 2811 の動作を説明する。

【0095】

予約証明証の検証の動作は予約証明証検証機器 2801 から始まる。

【0096】

まず、チャンレンジ生成部 2803 でチャレンジ C が作成される (2901)。チャンレンジは検証を行うたびに異なる乱数値であり、チャンレンジ生成部 2803 は乱数生成機能を内包している。

【0097】

チャレンジが生成された後、生成されたチャレンジ C、公開鍵情報記憶部 2804 に保持されている検証用公開鍵の識別子 ID と法数 n および公開鍵 e 、条件指定記憶部 2802 に保持されている条件指定 s が、携帯型記憶装置制御部 2806 を介して携帯型記憶装置 2811 に送付される (2902)。

【0098】

C, ID, n , e , s を受け取った携帯型記憶装置制御部 2806 は、まず予約証明証記憶部 2816 に保持されている予約証明証のうち検証用公開鍵識別子 ID に対応するものが選択される (2903)。この選択は、予約証明証記憶部 2816 に保持されている予約証明証のうち、その公開鍵識別子フィールドの値が ID と等しいかどうかを調べる事で行われる。ここで該当する予約証明証が見つからなければ、エラーが入出力制御部 2812 を介して予約証明証検証機器 2801 に送付され (2908)、終了する。

【0099】

該当する予約証明証が見つかった場合には、予約条件判定部 2815 で該予約証明証に含まれる予約条件 1 が満たされているかどうか判定される (2904)。予約条件 1 に記載されている予約証明証の有効期間開始や終了のチェックの

ために、予約条件判定部 2815 は時計を内蔵している。また、予約証明証検証機器 2801 から条件指定 s が入力されている場合、条件指定 s が予約条件 1 を満たすかどうかもここで判定される。たとえば、予約証明証検証機器 2801 がコンサート開場の座席に設置されており、その席の番号を予約条件に持つ予約証明証のみを正当であると判定したい場合には、条件指定として座席番号を条件指定記憶部 2802 に記憶しておき、 s として該番号を携帯型記憶装置 2811 に送付し、予約条件判定部 2815 で予約条件 1 が予約指定 s に記載されている座席番号を含むかどうかを検査すればよい。

【0100】

2904 で、予約条件 1 が満たされていないと判断された場合、エラーが入出力制御部 2812 を介して予約証明証検証機器 2801 に送付され、終了する (2908)。

【0101】

2904 で、予約条件 1 が満たされていると判断された場合、レスポンス計算部 2814 でレスポンス R が計算され (2905)、入出力制御部 2812 を介して予約証明証検証機器 2801 に送付される (2906)。レスポンス R は、入出力制御部 2812 を介して予約証明証検証機器 2801 から入力されたチャレンジ C 、法数 n 、公開鍵 e 、2903 で選択された予約証明証に含まれる予約値 t と予約条件 1、消費者秘密情報記憶部 2813 に保持されている消費者秘密情報 u から、以下の (2) 式にしたがって計算される。

【0102】

【数 2】

$$R = C^{t+f(n,e,u,i)} \bmod n \quad (2)$$

携帯型記憶装置制御部 2806 を介してレスポンス R を受け取った予約証明証検証機器 2801 は、レスポンス検査部 2805 でレスポンス R の正当性を検証する (2907)。検証にはレスポンス R の他に、チャレンジ生成部 2803 が生成したチャレンジ C 、公開鍵情報記憶部 2806 が記憶している法数 n 、公開鍵 e が使用される。(3) の式が成り立てば検証成功、そうでなければ失敗である。

【0103】

【数3】

$$C \equiv R^e \pmod{n} \quad (3)$$

(1) (2) (3) の式からわかるように、法数や公開鍵、予約値、予約条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なる物品やサービスの予約証明証を流用したり、他人の予約証明証を利用したり、予約条件を改竄したりといった攻撃は困難である。

【0104】

図30は、消費者が保持する携帯型記憶装置が演算機能を持っている場合の、該携帯型記憶装置と予約証明証の検証機器のもう一つの構成例を示した図である。

【0105】

図30において、3001は予約証明証検証機器、3011は予約証明証検証機器3001に接続される携帯型記憶装置である。予約証明証検証機器3001は、チャレンジと呼ぶ乱数値を携帯型記憶装置3011に送付し、携帯型記憶装置3011は受け取ったチャレンジからレスポンスと呼ぶ値を計算して出力し、予約証明証検証機器3001がレスポンスの正しさを検査する事で、携帯型記憶装置3011に保持されている予約証明証の正当性を検証する。図28の構成では、予約証明証に含まれている予約値や予約条件を使用したのは携帯型記憶装置であったが、図30の構成では、予約値や予約条件を使用するのは予約証明証検証機器である点が異なる。

【0106】

予約証明証検証機器3001は、チャレンジ生成部3002、条件指定記憶部3003、公開鍵情報記憶部3004、レスポンス検査部3005、予約条件判定部3006、予約証明証記憶部3007、携帯型記憶装置制御部3008から構成される。

【0107】

予約証明証検証機器3001の各部の役割を以下に示す。

【0108】

チャレンジ生成部 3002 : 携帯型記憶装置 3011 に送付するチャレンジを生成する。

条件指定記憶部 3003 : 予約証明証検証機器 3001 が、予約証明証に記載されている予約条件が特定の条件を満たす場合にのみ予約証明証の検証に成功するよう構成する場合、予約条件に関する指定が保持される。

公開鍵情報記憶部 3004 : この予約証明証検証機器に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

レスポンス検査部 3005 : 携帯型記憶装置 3011 が作成したレスポンスの正しさを検査する。

予約条件判定部 3006 : 予約証明証に記載されている予約条件が満たされているかどうかを判定する。

予約証明証記憶部 3007 : 携帯型記憶装置 3011 から取り出した予約証明証を保持する。

携帯型記憶装置制御部 3008 : 携帯型記憶装置 3011 との間の情報のやり取りを制御する。

【0109】

また、携帯型記憶装置 3011 は、入出力制御部 3012、消費者秘密情報記憶部 3013、レスポンス計算部 3014、予約証明証記憶部 3015 から構成される。

【0110】

携帯型記憶装置 3011 の各部の役割を以下に示す。

【0111】

入出力制御部 3012 : 予約証明証検証機器 3001 との間のデータの入出力を制御する。

消費者秘密情報記憶部 3013 : 消費者秘密情報を保持する。

レスポンス計算部 3014 : 予約証明証検証機器 3001 に送付するレスポンスを計算する。

予約証明証記憶部 3015 : 予約証明証が複数保持される。

【0112】

図31は、予約証明証の検証の際の予約証明証検証機器3001と携帯型記憶装置3011の動作を示すフローチャートである。図31に従って予約証明証の検証の際の予約証明証検証機器3001と携帯型記憶装置3011の動作を説明する。

【0113】

予約証明証の検証の動作は予約証明証検証機器3001から始まる。

【0114】

予約証明証検証機器3001は、携帯型記憶装置制御部3008を介して携帯型記憶装置3011の予約証明証記憶部3015にアクセスし、予約証明証記憶部3015に保持されている予約証明証のうち、予約証明証検証機器3001による予約証明証検証に使用可能なものを探す(3101)。予約証明証記憶部3015に保持されている予約証明証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部3004に保持されている検証用公開鍵識別子と一致するものが、求める予約証明証である。ここで該当する予約証明証が見つからなければ、予約証明証の検証は失敗であり、エラー処理の後(3109)、終了する。

【0115】

該当する予約証明証が見つかった場合には、該予約証明証が取り出され、予約証明証検証機器3001の予約証明証記憶部3007に記憶される(3102)。

【0116】

次に、予約条件判定部3006で、予約証明証記憶部3007に保持されている予約証明証に含まれる予約条件1が満たされているかどうか判定される(3103)。予約条件1に記載されている予約証明証の有効期間開始や終了のチェックのために、予約条件判定部3006は時計を内蔵している。また、条件指定記憶部3003に条件指定が保持されている場合、該条件指定が予約条件1を満たすかどうかここで判定される。たとえば、予約証明証検証機器3001がホテルの部屋のドアに設置されており、その部屋番号を予約条件に持つ予約証明証のみを正当であると判定したい場合には、条件指定として部屋番号を条件指定記憶部3003に記憶しておき、予約条件判定部3006で予約条件1が条件指定

記憶部 3 0 0 3 に保持されている部屋番号を含むかどうかを検査すればよい。

【0 1 1 7】

3 1 0 3 で、予約条件 1 が満たされていないと判断された場合、予約証明証の検証は失敗であり、エラー処理の後（3 1 0 9）、終了する。

【0 1 1 8】

3 1 0 3 で、予約条件 1 が満たされていると判断された場合、チャレンジ生成部 3 0 0 2 でチャレンジ C が作成される（3 1 0 4）。チャレンジは検証を行うたびに異なる乱数値であり、チャレンジ生成部 3 0 0 2 は乱数生成機能を内包している。

【0 1 1 9】

チャレンジが生成された後、生成されたチャレンジ C、公開鍵情報記憶部 3 0 0 4 に保持されている法数 n および公開鍵 e 、予約証明証記憶部 3 0 0 7 に記憶されている予約証明証が含む予約条件 1 が、携帯型記憶装置制御部 3 0 0 8 を介して携帯型記憶装置 3 0 1 1 に送付される（3 1 0 5）。

【0 1 2 0】

チャレンジを受け取った携帯型記憶装置 3 0 1 1 は、レスポンス計算部 3 0 1 4 でレスポンス R を計算し（3 1 0 6）、入出力制御部 3 0 1 2 を介して予約証明証検証機器 3 0 0 1 に送付される（3 1 0 7）。レスポンス R は、入出力制御部 3 0 1 2 を介して予約証明証検証機器 3 0 0 1 から入力されたチャレンジ C、法数 n 、公開鍵 e 、予約条件 1、消費者秘密情報記憶部 3 0 1 3 に保持されている消費者秘密情報 u から、以下の（4）式にしたがって計算される。

【0 1 2 1】

【数 4】

$$R = C^{f(n,e,u,l)} \bmod n \quad (4)$$

携帯型記憶装置制御部 3 0 0 8 を介してレスポンス R を受け取った予約証明証検証機器 3 0 0 1 は、レスポンス検査部 3 0 0 5 でレスポンス R の正当性を検証する（3 1 0 8）。検証にはレスポンス R の他に、チャレンジ生成部 3 0 0 2 が生成したチャレンジ C、公開鍵情報記憶部 3 0 0 4 が記憶している法数 n 、公開鍵 e 、予約証明証記憶部 3 0 0 7 が保持している予約証明証に含まれる予約値 t が

使用される。(5)の式が成り立てば検証成功、そうでなければ失敗である。

【0122】

【数5】

$$C \equiv (C^t R)^e \pmod{n} \quad (5)$$

(1) (4) (5)の式からわかるように、法数や公開鍵、予約値、予約条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なる物品やサービスの予約証明証を流用したり、他人の予約証明証を利用したり、予約条件を改竄したりといった攻撃は困難である。

【0123】

図32は、消費者が保持する携帯型記憶装置が演算機能を持っていない場合の、該携帯型記憶装置と予約証明証の検証機器の構成例を示した図である。

【0124】

図32において、3201は予約証明証検証機器、3211は予約証明証検証機器3201に接続される携帯型記憶装置である。予約証明証検証機器3201は、携帯型記憶装置3211が保持している予約証明証をとりだし、その正当性を検証する。

【0125】

予約証明証検証機器3201は、条件指定記憶部3202、予約条件判定部3203、公開鍵情報記憶部3204、予約値検査部3205、予約証明証記憶部3206、携帯型記憶装置制御部3207、消費者秘密情報記憶部3208から構成される。

【0126】

予約証明証検証機器3201の各部の役割を以下に示す。

【0127】

条件指定記憶部3202：予約証明証検証機器3201が、予約証明証に記載されている予約条件が特定の条件を満たす場合にのみ予約証明証の検証に成功する場合、予約条件に関する指定が保持される。

予約条件判定部3203：予約証明証に記載されている予約条件が満たされているかどうかを判定する。

公開鍵情報記憶部 3 2 0 4 : この予約証明証検証機器に割り当てられた検証用公開鍵の識別子と法数および公開鍵を保持する。

予約値検査部 3 2 0 5 : 予約証明証に記載されている予約値の正当性を検証する。

予約証明証記憶部 3 2 0 6 : 携帯型記憶装置 3 2 1 1 から取り出した予約証明証を保持する。

携帯型記憶装置制御部 3 2 0 7 : 携帯型記憶装置 3 2 1 1 との間の情報のやり取りを制御する。

消費者秘密情報記憶部 3 2 0 8 : 携帯型記憶装置 3 2 1 1 から取り出した消費者秘密情報を保持する。

【 0 1 2 8 】

また、携帯型記憶装置 3 2 1 1 は、入出力制御部 3 2 1 2、消費者秘密情報記憶部 3 2 1 3、予約証明証記憶部 3 2 1 4 から構成される。

【 0 1 2 9 】

携帯型記憶装置 3 2 1 1 の各部の役割を以下に示す。

【 0 1 3 0 】

入出力制御部 3 2 1 2 : 予約証明証検証機器 3 2 0 1 との間のデータの入出力を制御する。

消費者秘密情報記憶部 3 2 1 3 : 消費者秘密情報を保持する。

予約証明証記憶部 3 2 1 4 : 予約証明証が複数保持される。

【 0 1 3 1 】

図 3 3 は、予約証明証の検証の際の予約証明証検証機器 3 2 0 1 と携帯型記憶装置 3 2 1 1 の動作を示すフローチャートである。図 3 3 に従って予約証明証の検証の際の予約証明証検証機器 3 2 0 1 と携帯型記憶装置 3 2 1 1 の動作を説明する。

【 0 1 3 2 】

予約証明証検証機器 3 2 0 1 は、携帯型記憶装置制御部 3 2 0 7 を介して携帯型記憶装置 3 2 1 1 の予約証明証記憶部 3 2 1 4 にアクセスし、予約証明証記憶部 3 2 1 4 に保持されている予約証明証のうち、予約証明証検証機器 3 2 0 1 に

よる予約証明証検証に使用可能なものを探す(3301)。予約証明証記憶部3214に保持されている予約証明証のうち、その公開鍵識別子フィールドの値が公開鍵情報記憶部3204に保持されている検証用公開鍵識別子と一致するものが、求める予約証明証である。ここで該当する予約証明証が見つからなければ、予約証明証の検証は失敗であり、エラー処理の後(3306)、終了する。

【0133】

該当する予約証明証が見つかった場合には、該予約証明証が取り出され、予約証明証検証機器3201の予約証明証記憶部3206に記憶される(3302)。

【0134】

次に、予約条件判定部3203で、予約証明証記憶部3206に保持されている予約証明証に含まれる予約条件1が満たされているかどうか判定される(3303)。予約条件1に記載されている予約証明証の有効期間開始や終了のチェックのために、予約条件判定部3203は時計を内蔵している。また、条件指定記憶部3203に条件指定が保持されている場合、該条件指定が予約条件1を満たすかどうかここで判定される。

【0135】

3303で、予約条件1が満たされていないと判断された場合、予約証明証の検証は失敗であり、エラー処理の後(3306)、終了する。

【0136】

3303で、予約条件1が満たされていると判断された場合、携帯型記憶装置制御部3207を介して携帯型記憶装置3211の消費者秘密情報記憶部3213にアクセスし、消費者秘密情報記憶部3213に保持されている消費者秘密情報uを取り出し、予約証明証検証機器3201の消費者秘密情報記憶部3208に記憶する(3304)。

【0137】

最後に、予約値検査部3205で、予約証明証記憶部3206に保持されている予約証明証に含まれる予約値tの正当性を検証する(3305)。検証のために、予約値検査部3205は乱数rを生成し、公開鍵情報記憶部3204が記憶

している法数 n 、公開鍵 e 、予約証明証記憶部 3206 が保持している予約証明証に含まれる予約条件 l 、消費者秘密情報記憶部 3208 が保持している消費者秘密情報 u に対して (6) の式が成り立つかどうかを検査する。

【0138】

【数6】

$$r \equiv (r^{t+f(n,e,u,l)})^e \bmod n \quad (6)$$

(1) (6) の式からわかるように、法数や公開鍵、予約値、予約条件、消費者秘密情報の組み合わせが正しい時のみレスポンスの検証に成功する。検証用公開鍵が異なる物品やサービスの予約証明証を流用したり、他人の予約証明証を利用したり、予約条件を改竄したりといった攻撃は困難である。

【0139】

〔検証用公開鍵情報の発行〕

検証用公開鍵情報はプロバイダからの依頼によって、センタで作成され、依頼したプロバイダに送付される。依頼の際には、検証用公開鍵情報依頼というデータが送受信される。通常、発信者は依頼をするプロバイダであり受信者は依頼を受けるセンタであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに依頼を行ったりセンタの代わりに依頼を受けたりする場合には、プロバイダやセンタ以外のエンティティが発信者や受信者になってもよい。

【0140】

検証用公開鍵情報依頼のデータ構造を以下に示す。

【0141】

【表4】

検証用公開鍵情報依頼 ::= {

発信者フィールド,

受信者フィールド,

日時フィールド,

公開鍵仕様フィールド,

デジタル署名フィールド,

証明証フィールド

}

【0142】

発信者フィールド：この検証用公開鍵情報依頼の発信者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報依頼の受信者の識別子が記載される。受信者は通常予約証発行センタであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報依頼の作成日時が記載される。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する依頼者の要望が記載される。検証用公開鍵を使用するプロバイダの識別子、公開鍵暗号アルゴリズム、鍵長の情報がここに記述できる。

デジタル署名フィールド：この検証用公開鍵情報依頼の発信者によるこの検証用公開鍵情報依頼に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報依頼のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0143】

検証用公開鍵情報依頼を受け取ったセンタは、検証用公開鍵情報依頼に記載された公開鍵仕様にしたがって公開鍵ペアを作成し、検証用公開鍵情報を作成して依頼者であるプロバイダに渡す。依頼された検証用公開鍵情報を作成するかしないか、あるいは、指定された公開鍵仕様通りに公開鍵を作成するかどうかはセンタが決定できる。

【0144】

検証用公開鍵情報を引き渡す際には、検証用公開鍵情報送付というデータが送受信される。通常、発信者は検証用公開鍵情報を作成したセンタであり、受信者は発行された検証用公開鍵情報を使用するプロバイダであるが、インターネットに接続されたその他のエンティティがセンタの代わりに検証用公開鍵情報の送付を行ったり、プロバイダの代わりに検証用公開鍵情報を受け取ったりする場合には、センタやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【0145】

検証用公開鍵情報送付のデータ構造を以下に示す。

【0146】

【表 5】

検証用公開鍵情報送付 ::= {

発信者フィールド,
受信者フィールド,
日時フィールド,
検証用公開鍵情報フィールド,
デジタル署名フィールド,
証明証フィールド

}

【0147】

発信者フィールド：この検証用公開鍵情報送付の送付者の識別子が記載される。

発信者は通常予約証発行センタであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この検証用公開鍵情報送付の受信者の識別子が記載される。

受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この検証用公開鍵情報送付の作成日時が記載される。

検証用公開鍵情報フィールド：この検証用公開鍵情報送付で送られる検証用公開鍵情報が記載される。

デジタル署名フィールド：この検証用公開鍵情報送付の発信者によるこの検証用公開鍵情報送付に対するデジタル署名が記載される。

証明証フィールド：この検証用公開鍵情報送付のデジタル署名フィールド、およびこの検証用公開鍵情報送付に含まれる検証用公開鍵情報のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0148】

[予約証明証仲介許諾]

本実施例では、プロバイダとリテーラは独立に存立することが可能である。リテーラは多様なプロバイダが提供する多様な物品やサービスの予約販売を行うことが可能であるし、特定のプロバイダが自己の提供する物品やサービスを多くのリテーラに予約販売をしてもらうといったことも可能である。

【0149】

プロバイダにとっては、多くのリテーラに自己の商品を予約販売してもらうことは基本的には有利であるが、自分と取引のない信用度の低いリテーラに予約販売をされるのは、後のトラブルを招く可能性が高く許容できない。したがって、プロバイダは自己の物品やサービスを取り扱えるリテーラをコントロールする必要がある。

【0150】

このコントロール可能にするために、本実施例では予約証明証仲介許諾というデータを使用する。

【0151】

予約証明証仲介許諾はプロバイダが特定のリテーラに対して自己の特定の物品やサービスの予約販売を委託している事を証するデジタルデータであり、リテーラからの依頼を受けて作成され、依頼者に送付される。

【0152】

予約証明証仲介許諾のデータ構造を以下に示す。

【0153】

【表 6】

予約証明証仲介許諾：：＝ {

発行者フィールド,
受領者フィールド,
発行日フィールド,
予約証明証仲介許諾識別子フィールド,
有効期間開始日時フィールド,
有効期間終了日時フィールド,

公開鍵識別子フィールド,
予約条件限定情報フィールド,
デジタル署名フィールド
}

【0154】

発行者フィールド：この予約証明証仲介許諾の発行者であるプロバイダの識別子が記載される。

受領者フィールド：この予約証明証仲介許諾の受領者であるリテーラの識別子が記載される。

発行日フィールド：この予約証明証仲介許諾の発行日が記載される。

予約証明証仲介許諾識別子フィールド：この予約証明証仲介許諾にプロバイダが割り当てた識別子が記載される。

有効期間開始日時フィールド：この予約証明証仲介許諾の有効期間の開始日時が記載される。

有効期間終了日時フィールド：この予約証明証仲介許諾の有効期間の終了日時が記載される。

公開鍵識別子フィールド：この予約証明証仲介許諾によって予約証明証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

予約条件限定情報フィールド：予約証明証に記載される予約条件の範囲を限定する情報である予約条件限定情報が記載される。

デジタル署名フィールド：発行者であるプロバイダによるこの予約証明証仲介許諾全体に対するデジタル署名が記載される。

【0155】

予約条件限定情報フィールドに記載される予約条件限定情報によって、プロバイダはリテーラが発行する予約証明証に記載される予約条件を詳細にコントロールする事ができる。

【0156】

予約条件限定情報のデータ構造を以下に示す。

【0157】

【表 7】

予約条件限定情報： := {
 最短有効期間フィールド,
 最長有効期間フィールド,
 ...
 }

【0158】

最短有効期間フィールド：この予約証明証仲介許諾の受領者であるリテーラが仲介して発行される、公開鍵鍵識別子で指定された検証用公開鍵に対応する予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最低限度が記載される。該予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以上でなければならない。

最長有効期間フィールド：この予約証明証仲介許諾の受領者であるリテーラが仲介して発行される、公開鍵鍵識別子で指定された検証用公開鍵に対応する予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さの最長限度が記載される。該予約証明証の予約条件フィールドに記載される有効期間開始から有効期間終了までの間の長さは、ここに記載される値以下でなければならない。

【0159】

予約条件限定情報には、最短有効期間あるいは最長有効期間以外にも、この予約証明証仲介許諾の公開鍵鍵識別子フィールドで指定された検証用公開鍵とバインドされている物品やサービスに応じて種々の限定を設定する事が可能である。たとえば、公開鍵鍵識別子フィールドで指定された検証用公開鍵が特定の日時のコンサートでの座席の予約に対応するものであって、特定のリテーラが予約販売できる座席を限定したい場合には、予約販売を許す座席番号の集合を予約条件限定情報フィールドに記載すればよい。これにより、予約証明証の予約条件フィールドに記載される座席番号を限定することができる。

【0160】

[予約証明証仲介許諾の発行]

予約証明証仲介許諾はリテラからの依頼によって、プロバイダで作成され、依頼したリテラに送付される。依頼の際には、予約証明証仲介許諾依頼というデータが送受信される。通常、発信者は依頼をするリテラであり受信者は依頼を受けるプロバイダであるが、インターネットに接続されたその他のエンティティがリテラの代わりに依頼を行ったりプロバイダの代わりに依頼を受けたりする場合には、リテラやプロバイダ以外のエンティティが発信者や受信者になってもよい。

【0161】

予約証明証仲介許諾依頼のデータ構造を以下に示す。

【0162】

【表 8】

予約証明証仲介許諾依頼 ::= {

発信者フィールド,
受信者フィールド,
日時フィールド,
予約証明証仲介許諾仕様フィールド,
デジタル署名フィールド,
証明証フィールド
}

【0163】

発信者フィールド：この予約証明証仲介許諾依頼の発信者の識別子が記載される。発信者は通常リテラであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この予約証明証仲介許諾依頼の受信者の識別子が記載される。受信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この予約証明証仲介許諾依頼の作成日時が記載される。

予約証明証仲介許諾仕様フィールド：作成してもらう予約証明証仲介許諾に対す

る依頼者の要望を記載した予約証明証仲介許諾仕様が記載される。

デジタル署名フィールド：この予約証明証仲介許諾依頼の発信者によるこの予約証明証仲介許諾依頼に対するデジタル署名が記載される。

証明証フィールド：この予約証明証仲介許諾依頼のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0164】

予約証明証仲介許諾依頼の予約証明証仲介許諾仕様フィールドに記載される予約証明証仲介許諾仕様のデータ構造を以下に示す。

【0165】

【表9】

予約証明証仲介許諾仕様：：＝ {
 許諾者フィールド，
 被許諾者フィールド，
 公開鍵識別子フィールド，
 希望予約条件限定情報フィールド
 }

【0166】

許諾者フィールド：予約証明証仲介許諾を作成してほしいプロバイダの識別子が記載される。

被許諾者フィールド：希望する予約証明証仲介許諾によって許諾を受けるリテーラの識別子が記載される。

公開鍵識別子フィールド：予約証明証仲介許諾で予約証明証の仲介を許諾してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

希望予約条件限定情報フィールド：作成してもらう予約証明証仲介許諾に記載してほしい予約条件限定情報が記載される。

【0167】

予約証明証仲介許諾依頼を受け取ったプロバイダは、予約証明証仲介許諾依頼に記載された予約証明証仲介許諾仕様にしたがって予約証明証仲介許諾を作成し、リテーラに渡す。依頼された予約証明証仲介許諾を作成するかしないか、ある

いは、指定された予約証明証仲介許諾仕様どおりに予約証明証仲介許諾を作成するかどうかはプロバイダが決定できる。

【0168】

作成した予約証明証仲介許諾を引き渡す際には、予約証明証仲介許諾送付というデータが送受信される。通常、発信者は予約証明証仲介許諾を作成したプロバイダであり、受信者は発行された予約証明証仲介許諾を使用するリテーラであるが、インターネットに接続されたその他のエンティティがプロバイダの代わりに予約証明証仲介許諾の送付を行ったり、リテーラの代わりに予約証明証仲介許諾を受け取ったりする場合には、プロバイダやリテーラ以外のエンティティが発信者や受信者になってもよい。

【0169】

予約証明証仲介許諾送付のデータ構造を以下に示す。

【0170】

【表10】

予約証明証仲介許諾送付 ::= {

発信者フィールド,
受信者フィールド,
日時フィールド,
予約証明証仲介許諾フィールド,
デジタル署名フィールド,
証明証フィールド
}

【0171】

発信者フィールド：この予約証明証仲介許諾送付の送付者の識別子が記載される。発信者は通常プロバイダであるが、インターネットに接続された別のエンティティでもよい。

受信者フィールド：この予約証明証仲介許諾送付の受信者の識別子が記載される。受信者は通常リテーラであるが、インターネットに接続された別のエンティティでもよい。

日時フィールド：この予約証明証仲介許諾送付の作成日時が記載される。

予約証明証仲介許諾フィールド：この予約証明証仲介許諾送付で送られる予約証明証仲介許諾が記載される。

デジタル署名フィールド：この予約証明証仲介許諾送付の発信者によるこの予約証明証仲介許諾送付に対するデジタル署名が記載される。

証明証フィールド：この予約証明証仲介許諾送付のデジタル署名フィールド、およびこの予約証明証仲介許諾送付に含まれる予約証明証仲介許諾のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0172】

[予約証明証の発行]

予約証明証は、消費者からの依頼に応じて発行される。消費者はリテーラに対して特定の物品やサービスに対して特定の予約条件での予約を依頼する予約証明証依頼を送付する。予約証明証依頼を受け取ったリテーラは、通常センタに対して、依頼元である消費者に対する予約証明証の発行を依頼するため予約証明証依頼を作成し、センタに送付する。予約証明証依頼を受け取ったセンタは消費者向けの予約証明証を作成し、予約証明証依頼を送付してきたリテーラに渡す。予約証明証を受け取ったリテーラは、その予約証明証をその依頼者である消費者に送付する。センタからあるいはリテーラからの予約証明証の送付には、予約証明証送付というデータが送受信される。

【0173】

消費者とセンタの間を複数のリテーラが仲介することも可能である。その場合、消費者からの依頼を直接受けたリテーラが第2のリテーラに予約証明証依頼を送付し、第2のリテーラがセンタに予約証明証依頼を送付するという形態をとる。発行された予約証明証は逆の経路で予約証明証送付を送付していく事で消費者に届く。

【0174】

予約証明証依頼のデータ構造を以下に示す。

【0175】

【表 1 1】

予約証明証依頼： := {

発信者フィールド,
 受信者フィールド,
 日時フィールド,
 予約内容フィールド,
 デジタル署名フィールド,
 証明証フィールド
 }

【0 1 7 6】

発信者フィールド：この予約証明証依頼の発信者の識別子が記載される。

受信者フィールド：この予約証明証依頼の受信者の識別子が記載される。

日時フィールド：この予約証明証依頼の作成日時が記載される。

予約内容フィールド：依頼する予約証明証の内容に関する要望のためのフィールドである。通常、予約内容に関する要望を記した予約仕様が記載されるが、受信者がリテーラであって、リテーラで予約販売している物品あるいはサービスにリテーラ独自の管理番号が割り当ててある場合には、その番号が記載されることもある。

デジタル署名フィールド：この予約証明証依頼の発信者によるこの予約証明証依頼に対するデジタル署名が記載される。

証明証フィールド：この予約証明証依頼のデジタル署名フィールド、およびこの予約証明証依頼に予約証明証仲介許諾が含まれるならばそのデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

。

【0 1 7 7】

予約証明証依頼の予約内容フィールドに記載される予約仕様のデータ構造を以下に示す。

【0 1 7 8】

【表 1 2】

予約仕様 : : = {
 公開鍵識別子フィールド,
 消費者識別子フィールド,
 予約条件フィールド,
 予約証明証仲介許諾フィールド
 }

【0179】

公開鍵識別子フィールド：予約証明証依頼で依頼する予約証明証を検証できる
 検証用公開鍵に割り当てられた検証用公開鍵識別子が記載される。

消費者識別子フィールド：予約証明証依頼で依頼する予約証明証で予約を証され
 る消費者の識別子が記載される。

予約条件フィールド：予約証明証依頼で依頼する予約証明証に記載してほしい予
 約条件が記載あされる。

予約証明証仲介許諾フィールド：予約証明証依頼の発信者がリテラの場合に、
 そのリテラが、この予約仕様の公開鍵識別子フィールドに指定された識別子
 をもつ検証用公開鍵に対応する予約証明証を、この予約仕様の予約条件フィ
 ールドに記載された予約条件で依頼することの仲介が許諾されている事を証する予約
 証明証仲介許諾が含まれる。

【0180】

予約仕様の予約条件フィールドに記載されたとおりの予約条件を持つ予約証明
 証を発行するかどうかは、センタが決定する。特に、予約仕様に含まれる予約証
 明証仲介許諾で許諾されていない依頼に対しては、予約証明証を発行しない。

【0181】

また、予約証明証の依頼の過程で、仲介するリテラが予約仕様の予約条件フ
 ィールドの内容を修正する事もありうる。

【0182】

予約証明証送付のデータ構造を以下に示す。

【0183】

【表13】

予約証明証送付：：＝ {

発信者フィールド，
 受信者フィールド，
 日時フィールド，
 予約証明証フィールド，
 デジタル署名フィールド，
 証明証フィールド
 }

【0184】

発信者フィールド：この予約証明証送付の送付者の識別子が記載される。

受信者フィールド：この予約証明証送付の受信者の識別子が記載される。

日時フィールド：この予約証明証送付の作成日時が記載される。

予約証明証フィールド：この予約証明証送付で送られる予約証明証が記載される。

デジタル署名フィールド：この予約証明証送付の発信者によるこの予約証明証仲介許諾送付に対するデジタル署名が記載される。

証明証フィールド：この予約証明証送付のデジタル署名フィールド、およびこの予約証明証送付に含まれる予約証明証のデジタル署名フィールドのデジタル署名を検証するための公開鍵を含む公開鍵証明証群が記載される。

【0185】

[センタの構成]

本実施例のセンタは、インターネットを介して入力される検証用公開鍵情報依頼と予約証明証依頼を処理する機能、予約証明証の発行履歴を作成してインターネットを介してプロバイダあるいはリテーラに送付する機能、検証用公開鍵情報の発行履歴を作成してインターネットを介してプロバイダに送付する機能を持つ。

【0186】

図2は、本実施例のセンタの構成図である。

【0187】

センタは、入出力制御部201、処理選択部202、検証用公開鍵情報依頼処理部203、予約証明証依頼処理部204、プロバイダDB205、公開鍵ペアDB206、リテラDB207、消費者DB208、予約証明証発行履歴DB209、署名鍵記憶部210、証明証記憶部211、予約証明証発行プロバイダ用履歴作成部212、予約証明証発行リテラ用履歴作成部213、検証用公開鍵情報発行履歴作成部214から構成され、入出力制御部201を介してインターネットに接続されている。

【0188】

本実施例のセンタの各部の役割を以下に述べる。

【0189】

入出力制御部201：インターネットを介したデータの入力を受け付けるとともに、検証用公開鍵情報依頼処理部203が作成したデータや予約証明証依頼処理部204が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部201への入力、あるいは、入出力制御部201からインターネットへの出力の方法としては、入出力制御部201と接続されたWWWサイトを準備してプロバイダやリテラにアクセスさせるもの、あるいは電子メールシステムと入出力制御部201を自動的にあるいは人手によって連動させるものなど可以使用。

処理選択部202：入力したデータが検証用公開鍵情報依頼かまたは予約証明証依頼かを判断し、検証用公開鍵情報依頼であれば検証用公開鍵情報依頼処理部203を、予約証明証依頼であれば予約証明証依頼処理部204を呼び出す。

検証用公開鍵情報依頼処理部203：検証用公開鍵情報依頼を処理し、検証用公開鍵情報依頼送付を作成して入出力制御部201を介して依頼者に送付する。検証用公開鍵情報依頼送付作成の過程で、プロバイダDB205を参照するとともに、公開鍵ペアDB206に新しいエントリを追加する。

予約証明証依頼処理部204：予約証明証依頼を処理し、予約証明証依頼送付を作成して入出力制御部201を介して依頼者に送付する。予約証明証依頼送付作成の過程で、公開鍵ペアDB206、リテラDB207、消費者DB208を参照するとともに、予約証明証発行履歴DBに新しいエントリを追加する。

プロバイダDB205：プロバイダに関するデータを保持するDB。

公開鍵ペアDB206：検証用公開鍵情報あるいは予約証明証の作成に使用される公開鍵ペアを保持するDB。

リテラDB207：リテラに関するデータを保持するDB。

消費者DB208：消費者に関するデータを保持するDB。

予約証明証発行履歴DB209：予約証明証の発行履歴に関するデータを保持するDB。

署名鍵記憶部210：センタが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部211：署名鍵記憶部210に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

予約証明証発行プロバイダ用履歴作成部212：各プロバイダ毎の予約証明証の発行履歴を作成し、入出力制御部201を介してプロバイダに送付する。

予約証明証発行リテラ用履歴作成部213：各リテラ毎の予約証明証の発行履歴を作成し、入出力制御部201を介してリテラに送付する。

検証用公開鍵情報発行履歴作成部214：各プロバイダ毎の検証用公開鍵情報の発行履歴を作成し、入出力制御部201を介してプロバイダに送付する。

【0190】

[センタが持つデータベース]

センタは、プロバイダDB205、公開鍵ペアDB206、リテラDB207、消費者DB208、予約証明証発行履歴DB209の5つのデータベースを持っている。

【0191】

プロバイダDB205は、センタがプロバイダとして認めているエンティティに関する情報を保持したデータベースである。

【0192】

プロバイダDB205の構造を図6に示す。プロバイダDB205は以下の唯一の属性からなるテーブルである。

【0193】

【表 14】

プロバイダ識別子属性：センタがプロバイダとして認めているエンティティの識別子。

【0194】

センタは、このデータベースに登録されているプロバイダ以外のエンティティをプロバイダとは認めない。したがって、そのようなエンティティに対して検証用公開鍵情報を発行することはないし、そのようなエンティティが提供している物品やサービスに対する予約証明証を発行する事もない。

【0195】

センタがプロバイダと認めるエンティティを増やしたい場合には、このデータベースに新規エントリを追加する。

【0196】

公開鍵ペアDB 206は、プロバイダに発行される検証用公開鍵と、それに対応する秘密鍵に関する情報を保持したデータベースである。本実施例では、検証用公開鍵とそれに対応する秘密鍵のための公開鍵暗号アルゴリズムとしてRSAを使用する。したがって、公開鍵ペアDB 206はRSAの公開鍵ペアについての情報を保持するデータベースである。

【0197】

公開鍵ペアDB 206の構造を図7に示す。公開鍵ペアDB 206は以下の7つの属性からなるテーブルであり、各エントリはそれぞれ一つの公開鍵ペアに関する情報である。

【0198】

【表 15】

公開鍵識別子属性：このエントリの公開鍵ペアに割り当てられた検証用公開鍵識別子。

法数属性：RSA法数。

公開鍵属性：RSA公開鍵。

秘密鍵属性：RSA秘密鍵。

プロバイダ識別子属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵

情報を発行されたプロバイダの識別子。

有効期間開始属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の有効期間の終了日時。

発行日属性：このエントリの公開鍵ペアの公開鍵を含む検証用公開鍵情報の発行日時。

【0199】

リテラDB207は、センタがリテラとして認めているエンティティに関する情報を保持したデータベースである。

【0200】

リテラDB207の構造を図8に示す。リテラDB207は以下の唯一の属性からなるテーブルである。

【0201】

【表16】

リテラ識別子属性：センタがリテラとして認めているエンティティの識別子

。

【0202】

センタは、このデータベースに登録されているリテラ以外のエンティティをリテラとは認めない。したがって、そのようなエンティティからの予約証明証発行依頼に対して予約証明証を発行する事はない。

【0203】

センタがリテラと認めるエンティティを増やしたい場合には、このデータベースに新規エントリを追加する。

【0204】

消費者DB208は、センタが消費者として認めているエンティティに関する情報を保持したデータベースである。

【0205】

消費者DB208の構造を図9に示す。消費者DB208は以下の2つの属性

からなるテーブルである。

【0206】

【表17】

消費者識別子属性：センタが消費者として認めているエンティティの識別子。消費者が所持する携帯型記憶装置の中にも保持されている値である。

消費者秘密情報属性：消費者識別子属性で指定された消費者識別子を保持している携帯型記憶装置内に保持されている消費者秘密情報。

【0207】

予約証明証発行履歴DB209は、センタがこれまでに発行した予約証明証に関する情報を保持したデータベースである。

【0208】

予約証明証発行履歴DB209の構造を図10に示す。予約証明証発行履歴DB209は以下の6つの属性からなるテーブルであり、各エントリはそれぞれ一つの予約証明証に関する情報である。

【0209】

【表18】

公開鍵識別子属性：このエントリの予約証明証を検証できる検証用公開鍵に割り当てられた検証用公開鍵識別子。

プロバイダ識別子属性：このエントリの公開鍵識別子属性で指定された検証用公開鍵を含む検証用公開鍵情報の発行を受けたプロバイダの識別子。

消費者識別子属性：このエントリの予約証明証で予約を証された消費者が持つ携帯型記憶装置に含まれる消費者識別子。

仲介者識別子属性：このエントリの予約証明証の発行を依頼したリテーラの識別子。

予約条件属性：このエントリの予約証明証に記載された予約条件をBER (Basic Encoding Rule: ITU-T Recommendation X.690) にしたがってエンコードした結果。

発行日属性：このエントリの予約証明証の発行日時。

【0210】

図3は、本実施例のセンタの動作を示すフローチャートである。本実施例のセンタの動作を図3のフローチャートにしたがって説明する。

【0211】

図3に示す通り、本実施例のセンタは、データの入力を待ち続け、入力があれば入力に応じた処理を行った後に再度入力待ちの状態に戻る終わる事のない処理である。

【0212】

最初に、入出力制御部201で入力があるかどうかチェックされる(301)。ここで入力がなければ、再度入力のチェック(301)に戻る。

【0213】

入力のチェック(301)で入力があった場合、処理選択部202で、その入力が検証用公開鍵情報依頼かどうか判断される(302)。入力が検証用公開鍵情報依頼であれば、検証用公開鍵情報依頼処理部203が呼び出され検証用公開鍵情報依頼が処理される(303)。検証用公開鍵情報依頼の処理が終われば、再度入力のチェック(301)に戻る。

【0214】

302の判断で、入力が検証用公開鍵情報依頼でなければ、処理選択部202で、その入力が予約証明証依頼かどうか判断される(304)。入力が予約証明証依頼であれば、予約証明証依頼処理部204が呼び出され予約証明証依頼が処理される(305)。予約証明証依頼の処理が終われば、再度入力のチェック(301)に戻る。

【0215】

また、304の判断で、入力が予約証明証依頼でなければ、再度入力のチェック(301)に戻る。

【0216】

[検証用公開情報依頼処理部]

図4は、本実施例のセンタが持つ検証用公開情報依頼処理部203の内部構成を示した図である。

【0217】

検証用公開情報依頼処理部 203 は、検証用公開情報依頼を処理する機能を持ち、処理制御部 401、署名検証部 402、公開鍵ペア作成部 403、公開鍵ペア識別子作成部 404、検証用公開鍵情報作成部 405、検証用公開鍵情報送付作成部 406、エラーメッセージ作成部 407、署名作成部 408 から構成される。

【0218】

検証用公開情報依頼処理部 203 を構成する各部の役割を以下に述べる。

【0219】

処理制御部 401：処理選択部 202 からの入力、入出力制御部 201 への出力、プロバイダ DB 205 の参照、公開鍵ペア DB 206 へのエントリの追加の機能を担うとともに、検証用公開情報依頼の処理全体を制御する。

署名検証部 402：処理選択部 202 から入力される検証用公開情報依頼のデジタル署名を検証する。

公開鍵ペア作成部 403：検証用公開鍵および予約証明証の作成に使用される公開鍵ペアを作成する。

公開鍵ペア識別子作成部 404：検証用公開鍵に割り当てられる検証用公開鍵識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

検証用公開鍵情報作成部 405：検証用公開鍵情報を作成する。検証用公開鍵情報にデジタル署名を添付するために署名作成部 408 を呼び出す。

検証用公開鍵情報送付作成部 406：検証用公開鍵情報送付を作成する。検証用公開鍵情報送付にデジタル署名を添付するために署名作成部 408 を呼び出す。

さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 211 にアクセスする。

エラーメッセージ作成部 407：エラーメッセージを作成する。

署名作成部 408：検証用公開鍵情報、検証用公開鍵情報送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 210 にアクセスする。

【0220】

図 5 は、本実施例のセンタが持つ検証用公開情報依頼処理部 2 0 3 の処理制御部 4 0 1 の動作を示すフローチャートである。処理制御部 4 0 1 の動作を図 5 にしたがって説明する。

【 0 2 2 1 】

まず、処理選択部 2 0 2 から入力された検証用公開情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子を取り出し、センタがこの識別子のエンティティをプロバイダとして認めているかどうかをプロバイダ DB 2 0 5 を参照して調べる (5 0 1) 。プロバイダ DB 2 0 5 にこの識別子を持つエントリが存在すれば、プロバイダとして認めたエンティティであることがわかる。

【 0 2 2 2 】

5 0 1 の判断で、プロバイダとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部 4 0 7 でエラーメッセージを作成して入出力制御部 2 0 1 に出力した後 (5 0 9) 、終了する。

【 0 2 2 3 】

5 0 1 の判断で、プロバイダとして認めているエンティティであることがわかった場合、検証用公開情報依頼のデジタル署名を検証する (5 0 2) 。検証鍵は検証用公開情報依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA 1 1 1 から公開鍵証明証を取得してから署名の検証を行う。

【 0 2 2 4 】

署名の検証に失敗した場合、エラーメッセージ作成部 4 0 7 でエラーメッセージを作成して入出力制御部 2 0 1 に出力した後 (5 0 9) 、終了する。

【 0 2 2 5 】

署名の検証に成功した場合、公開鍵ペア作成部 4 0 3 を呼び出して RSA 公開鍵ペアを作成させ、作成された法数、公開鍵、秘密鍵を受け取る (5 0 3) 。さらに、公開鍵ペア識別子作成部 4 0 4 を呼び出して検証用公開鍵情報に割り当てる識別子を作成させ、作成された識別子を受け取る (5 0 4) 。

【 0 2 2 6 】

次に検証用公開鍵情報の有効期間の開始日時と終了日時を適切に決定した後（505）、新しいエントリを公開鍵ペアDBに追加する（506）。新しいエントリの各属性には以下の値が設定される。

【0227】

【表19】

公開鍵識別子属性：504で作成した識別子。

法数属性：503で作成したRSA法数。

公開鍵属性：503で作成したRSA公開鍵。

秘密鍵属性：503で作成したRSA秘密鍵。

プロバイダ識別子属性：検証用公開情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

有効期間開始属性：505で作成した有効期間の開始日時。

有効期間終了属性：505で作成した有効期間の終了日時。

発行日属性：現在の日時。

【0228】

次に、検証用公開鍵情報作成部（405）を呼び出し、検証用公開鍵情報を作成させ、その結果を受け取る（507）。検証用公開鍵情報の各フィールドには以下の値が設定される。

【0229】

【表20】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：検証用公開情報依頼の公開鍵仕様フィールドに含まれる検証用公開鍵の使用者であるプロバイダの識別子。

発行日フィールド：現在の時刻。

有効期間開始日時フィールド：505で作成した有効期間の開始日時。

有効期間終了日時フィールド：505で作成した有効期間の終了日時。

検証用公開鍵鍵識別子フィールド：504で作成した識別子。

公開鍵情報フィールド：503で作成した法数、公開鍵、秘密鍵。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデ

デジタル署名。デジタル署名の作成のため、署名作成部 4 0 8 を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【0 2 3 0】

最後に、検証用公開鍵情報送付作成部 4 0 6 を呼び出し、検証用公開鍵情報送付を作成させ、その結果を受け取って入出力制御部 2 0 1 に出力した後（5 0 8）、終了する。検証用公開鍵情報送付の各フィールドには以下の値が設定される。

【0 2 3 1】

【表 2 1】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：検証用公開情報依頼の発信者フィールドに記載されている識別子。

日時フィールド：現在の時刻。

検証用公開鍵情報フィールド：5 0 7 で作成した検証用公開鍵情報。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部 4 0 8 を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部 2 1 1 に記憶している公開鍵証明証。

【0 2 3 2】

【予約証明証依頼処理部】

図 1 1 は、本実施例のセンタが持つ予約証明証依頼処理部 2 0 4 の内部構成を示した図である。

【0 2 3 3】

予約証明証依頼処理部 2 0 4 は、予約証明証依頼を処理する機能を持ち、処理制御部 1 1 0 1、署名検証部 1 1 0 2、予約証明証仲介許諾内容確認部 1 1 0 3、予約証明証識別子作成部 1 1 0 4、予約証明証作成部 1 1 0 5、予約証明証送付作成部 1 1 0 6、エラーメッセージ作成部 1 1 0 7、署名作成部 1 1 0 8、予約値作成部 1 1 0 9、予約条件作成部 1 1 1 0 から構成される。

【0 2 3 4】

予約証明証依頼処理部 204 を構成する各部の役割を以下に述べる。

【0235】

処理制御部 1101：処理選択部 202 からの入力、入出力制御部 201 への出力、公開鍵ペア DB 206 リテラ DB 207 消費者 DB 208 の参照、予約証明証発行履歴 DB 209 へのエントリの追加の機能を担うとともに、予約証明証依頼の処理全体を制御する。

署名検証部 1102：処理選択部 202 から入力される予約証明証依頼、および該予約証明証依頼に含まれる予約証明証仲介許諾のデジタル署名を検証する。

予約証明証仲介許諾内容確認部 1103：処理選択部 202 から入力される予約証明証依頼で依頼された予約証明証の仲介が、該予約証明証依頼に含まれている予約証明証仲介許諾によって許諾されているかどうかを確認する。

予約証明証識別子作成部 1104：予約証明証に割り当てられる予約証明証識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

予約証明証作成部 1105：予約証明証を作成する。予約証明証にデジタル署名を添付するために署名作成部 1108 を呼び出す。

予約証明証送付作成部 1106：予約証明証送付を作成する。予約証明証送付にデジタル署名を添付するために署名作成部 1108 を呼び出す。さらに、センタの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 211 にアクセスする。

エラーメッセージ作成部 1107：エラーメッセージを作成する。

署名作成部 1108：予約証明証、予約証明証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 210 にアクセスする。

予約値作成部 1109：予約証明証に含まれる予約値を作成する。

予約条件作成部 1110：予約証明証に含まれる予約条件を作成する。

【0236】

図 12 は、本実施例のセンタが持つ予約証明証依頼処理部 204 の処理制御部 1101 の動作を示すフローチャートである。処理制御部 1101 の動作を図 1

2にしたがって説明する。

【0237】

まず、処理選択部202から入力された予約証明証依頼の発信者フィールドに記載されている識別子を取り出し、センタがこの識別子のエンティティをリテラとして認めているかどうかをリテラDB207を参照して調べる(1201)。リテラDB207にこの識別子を持つエントリが存在すれば、リテラとして認めたエンティティであることがわかる。

【0238】

1201の判断で、リテラとして認めていないエンティティであることがわかった場合、エラーメッセージ作成部1107でエラーメッセージを作成して入出力制御部201に出力した後(1210)、終了する。

【0239】

1201の判断で、リテラとして認めているエンティティであることがわかった場合、予約証明証依頼のデジタル署名、および予約証明証依頼に含まれる予約証明証仲介許諾のデジタル署名を検証する(1202)。検証鍵は予約証明証依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA111から公開鍵証明証を取得してから署名の検証を行う。

【0240】

署名の検証に失敗した場合、エラーメッセージ作成部1107でエラーメッセージを作成して入出力制御部201に出力した後(1210)、終了する。

【0241】

署名の検証に成功した場合、予約証明証依頼で依頼された予約証明証の仲介が、該予約証明証依頼に含まれている予約証明証仲介許諾によって許諾されているかどうかを確認する(1203)。より具体的には、予約証明証依頼の予約内容フィールドに含まれている予約仕様を予約証明証仲介許諾内容確認部1103に送付し、該予約仕様の公開鍵識別子フィールドで指定されている検証用公開鍵識別子を持つ検証用公開鍵に対応する予約証明証を、該予約仕様の予約条件フィールドに記載されている予約条件で発行することが、該予約仕様の予約証明証仲

介許諾フィールドに含まれている予約証明証仲介許諾で許諾されているかどうかを確認する。

【0242】

1203で、許諾されていない事がわかった場合、エラーメッセージ作成部1107でエラーメッセージを作成して入出力制御部201に出力した後（1210）、終了する。

【0243】

1203で、許諾されている事がわかった場合、予約証明証識別子作成部1104を呼び出して予約証明証に割り当てる識別子を作成させ、作成された識別子を受け取った後（1204）、予約条件作成部1110を呼び出して、予約証明証に記載する予約条件を決定する（1205）。予約条件作成部が生成する予約条件は、予約証明証依頼予約内容フィールドに含まれている予約仕様の予約条件フィールドの値そのままでもよいし、該予約仕様の予約証明証仲介許諾フィールドに含まれている予約証明証仲介許諾によって許諾されている範囲内で該予約条件フィールドの値を適切に修正してもよい。

【0244】

予約条件の作成の後、新しいエントリを予約証明証発行履歴DB209に追加する（1206）。新しいエントリの各属性には以下の値が設定される。

【0245】

【表22】

公開鍵識別子属性：予約証明証依頼の予約内容フィールドに含まれている予約仕様の公開鍵識別子フィールドの値。

プロバイダ識別子属性：公開鍵ペアDBにアクセスし、該公開鍵ペアDBの公開鍵識別子属性が、予約証明証依頼の予約内容フィールドに含まれている予約仕様の公開鍵識別子フィールドの値と同じ値を持つエントリの、プロバイダ識別子属性を取り出し、その値を設定する。

消費者識別子属性：予約証明証依頼の予約内容フィールドに含まれている予約仕様の消費者識別子フィールドの値。

仲介者識別子属性：予約証明証依頼の発信者フィールドの値。

予約条件属性：1205で予約条件作成部が作成した予約条件。

発行日属性：現在の日時。

【0246】

次に、予約値作成部1109を呼び出して予約値を作成させ、その結果を受け取る（1207）。

【0247】

次に、予約証明証作成部1105を呼び出し、予約証明証を作成させ、その結果を受け取る（1208）。予約証明証の各フィールドには以下の値が設定される。

【0248】

【表23】

発行者フィールド：自分自身すなわちセンタの識別子。

受領者フィールド：予約証明証依頼の予約内容フィールドに含まれている予約仕様の消費者識別子フィールドの値。

発行日フィールド：1206で予約証明証発行履歴DB209に追加したエントリの発行日属性の値。

予約証明証識別子フィールド：1204で作成した識別子。

公開鍵識別子フィールド：予約証明証依頼の予約内容フィールドに含まれている予約仕様の公開鍵識別子フィールドの値。

予約条件フィールド：1205で予約条件作成部が作成した予約条件。

予約値フィールド：1207で作成した予約値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1108を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【0249】

最後に、予約証明証送付作成部1106を呼び出し、予約証明証送付を作成させ、その結果を受け取って入出力制御部201に出力した後（1209）、終了する。予約証明証送付の各フィールドには以下の値が設定される。

【0250】

【表 2 4】

発信者フィールド：自分自身すなわちセンタの識別子。

受信者フィールド：予約証明証依頼の発信者フィールドの値。

日時フィールド：現在の時刻。

予約証明証フィールド：1208で作成した予約証明証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1108を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部211に記憶している公開鍵証明証。

【0251】

[センタが持つその他の機能]

本実施例のセンタは、予約証明証発行の履歴情報をプロバイダに送付することができる。

【0252】

プロバイダに渡される予約証明証発行の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する予約証明証の発行についての情報であり、予約証明証発行プロバイダ用履歴作成部212で作成され、入出力制御部201を介してプロバイダに送付される。プロバイダにとっては、この履歴情報は、自己が提供している物品やサービスをどのリテーラがどのくらい予約販売したかのを示す信頼できる情報であり、予約販売におけるマージンがリテーラからプロバイダに渡される場合に、リテーラから送られたマージンの正しさをプロバイダが確認する際の重要な情報となる。

【0253】

予約証明証発行プロバイダ用履歴作成部212は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証発行履歴DB209から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、仲介者識別子属性、予約条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子

と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【0254】

本実施例のセンタは、予約証明証発行の履歴情報をリテーラにも送付することができる。

【0255】

リテーラに渡される予約証明証発行の履歴情報は、そのリテーラからの依頼で行った予約証明証の発行についての情報であり、予約証明証発行リテーラ用履歴作成部213で作成され、入出力制御部201を介してリテーラに送付される。この履歴は、センタがリテーラから予約証明証発行のマージンを受け取る場合のマージンの額の根拠となる。

【0256】

予約証明証発行リテーラ履歴作成部213は、履歴を作成するリテーラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証発行履歴DB209から、仲介者識別子属性の値が指定されたりテーラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、予約条件属性、発行日属性の値を取り出す。本実施例では、履歴を作成するリテーラの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でリテーラから入力されるように構成してもよい。

【0257】

また、本実施例のセンタは、検証用公開鍵情報発行の履歴情報をプロバイダに送付することができる。

【0258】

プロバイダに渡される検証用公開鍵情報発行の履歴情報は、そのプロバイダに対して発行された検証用公開鍵情報についての情報であり、検証用公開鍵情報発行履歴作成部214で作成され、入出力制御部201を介してプロバイダに送付される。この履歴は、センタがプロバイダから検証用公開鍵情報発行の手数料を徴収する場合の根拠となる。

【0259】

検証用公開鍵情報発行履歴作成部214は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、公開鍵ペアDB206から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発効日属性の値が指定された履歴作成の対象期間内であるエントリ郡を取り出し、その公開鍵識別子属性、法数属性、公開鍵属性、有効期間開始属性、有効期間終了属性、発行日属性の値を取り出す。本実施例では、履歴を作成するプロバイダの識別子と履歴作成の対象期間の指定はセンタのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【0260】

上記の履歴情報のプロバイダやリテーラへの送付方法は、電子メールでもよいし、WWWベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【0261】

[プロバイダの構成]

図13は、本実施例のプロバイダの構成図である。

【0262】

本実施例のプロバイダは、検証用公開鍵情報依頼を作成してインターネットを介してセンタに送付する機能と、インターネットを介して入力される検証用公開鍵情報送付と予約証明証仲介許諾依頼とを処理する機能を持つ。プロバイダは、入出力制御部1301、処理選択部1302、検証用公開鍵情報依頼作成部1303、検証用公開鍵情報送付処理部1304、予約証明証仲介許諾依頼処理部1305、検証用公開鍵DB1306、署名鍵記憶部1307、証明証記憶部1308、予約証明証仲介許諾発行履歴DB1309、予約証明証仲介許諾発行履歴作成部1310から構成され、入出力制御部1301を介してインターネットに接続されている。

【0263】

本実施例のプロバイダの各部の役割を以下に述べる。

【0264】

入出力制御部1301：インターネットを介したデータの入力を監視するとともに、検証用公開鍵情報依頼作成部1303や予約証明証仲介許諾依頼処理部1305が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部1301への入力、あるいは、入出力制御部1301からインターネットへの出力の方法としては、入出力制御部1301と接続されたWWWサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているWWWサイトにアクセスしてプロバイダが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部1301を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部1302：入力したデータが検証用公開鍵情報送付かまたは予約証明証仲介許諾依頼かを判断し、検証用公開鍵情報送付であれば検証用公開鍵情報送付処理部1304を、予約証明証仲介許諾依頼であれば予約証明証仲介許諾依頼処理部1305を呼び出す。

検証用公開鍵情報依頼作成部1303：検証用公開鍵情報依頼を作成し、入出力制御部1301を介してセンタに送付する。検証用公開鍵情報依頼作成の過程で、署名鍵記憶部1307と証明証記憶部1308にアクセスする。

検証用公開鍵情報送付処理部1304：検証用公開鍵情報送付を処理し、検証用公開鍵を検証用公開鍵DB1306に登録する。

予約証明証仲介許諾依頼処理部1305：予約証明証仲介許諾依頼を処理し、予約証明証仲介許諾送付を作成して入出力制御部1301を介して依頼者に送付する。予約証明証仲介許諾送付作成の過程で検証用公開鍵DB1306を参照し、予約証明証仲介許諾DBに新しいエントリを追加するとともに、署名鍵記憶部1307と証明証記憶部1308にアクセスする。

検証用公開鍵DB1306：検証用公開鍵に関する情報を保持するDB。

署名鍵記憶部1307：プロバイダが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部1308：署名鍵記憶部1307に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

予約証明証仲介許諾発行履歴DB1309：予約証明証仲介許諾の発行の履歴を

保持するDB。

予約証明証仲介許諾発行履歴作成部 1310：リテラ毎の予約証明証仲介許諾の発行履歴を作成する。

【0265】

[プロバイダが持つデータベース]

プロバイダは、検証用公開鍵DB 1306、予約証明証仲介許諾発行履歴DB 1309の2つのデータベースを持っている。

【0266】

検証用公開鍵DB 1306は、センタから発行を受けた検証用公開鍵情報の内容を、プロバイダ自身が決定した検証用公開鍵の用途とともに保持するデータベースである。

【0267】

検証用公開鍵DB 1306の構造を図14に示す。検証用公開鍵DB 1306は以下の6つの属性からなるテーブルであり、各エントリはそれぞれ一つの検証用公開鍵に関する情報である。

【0268】

【表25】

公開鍵識別子属性：検証用公開鍵に割り当てられた検証用公開鍵識別子。

法数属性：検証用公開鍵情報に含まれていたRSA法数。

公開鍵属性：検証用公開鍵情報に含まれていたRSA公開鍵。

有効期間開始属性：検証用公開鍵情報の有効期間の開始日時。

有効期間終了属性：検証用公開鍵情報の有効期間の終了日時。

用途属性：このエントリの検証用公開鍵に対してプロバイダが割り当てた用途。この検証用公開鍵で予約証明証の正当性を検証する物品やサービスの情報である。

【0269】

予約証明証仲介許諾発行履歴DB 1309は、プロバイダが発行した予約証明証仲介許諾に関する履歴を保持するデータベースである。

【0270】

予約証明証仲介許諾発行履歴DB1309の構造を図34に示す。予約証明証仲介許諾発行履歴DB1309は以下の7つの属性からなるテーブルであり、各エントリはそれぞれ一回の予約証明証仲介許諾の発行に関する情報である。

【0271】

【表26】

予約証明証仲介許諾識別子属性：発行した予約証明証仲介許諾に割り当てられた識別子。

公開鍵識別子属性：発行した予約証明証仲介許諾で予約証明証の仲介が許諾される検証用公開鍵に割り当てられた検証用公開鍵識別子。

リテラ識別子属性：発行した予約証明証仲介許諾で許諾をうけるリテラの識別子。

予約条件限定情報属性：発行した予約証明証仲介許諾に記載されている予約条件限定情報。

有効期間開始属性：発行した予約証明証仲介許諾の有効期間の開始日時。

有効期間終了属性：発行した予約証明証仲介許諾の有効期間の終了日時。

発行日属性：発行した予約証明証仲介許諾の発行日時。

【0272】

【検証用公開鍵情報依頼作成部】

本実施例のプロバイダは、新たに予約販売を開始したい物品やサービスが発生した時に、その物品やサービスに割り当てる検証用公開鍵を含む検証用公開鍵情報の発行をセンタに依頼する。依頼の際には、検証用公開鍵情報依頼作成部1303において検証用公開鍵情報依頼を作成し、入出力制御部1301を介してセンタに送付する。

【0273】

検証用公開鍵情報依頼作成部1303では、検証用公開鍵情報依頼の各フィールドに以下の値を設定する。

【0274】

【表27】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の時刻。

公開鍵仕様フィールド：作成してもらう検証用公開鍵に対する要望。検証用公開鍵の使用者として自分の識別子を記載し、さらに、要望する公開鍵暗号アルゴリズムと鍵長が記載される。本実施例では公開鍵暗号アルゴリズムとしてはRSAのみが仕様可能なので、公開鍵暗号アルゴリズムの値はRSAで固定である。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、検証用公開鍵情報依頼作成部1303は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部1307にアクセスして入手する。

【0275】

【表28】

証明証フィールド：証明証記憶部1308に記憶している公開鍵証明証。

【0276】

〔検証用公開鍵情報送付処理部〕

検証用公開鍵情報依頼作成部1303で検証用公開鍵情報依頼が作成されセンタに送付されると、その返信としてセンタから検証用公開鍵情報送付が送信されてくる。検証用公開鍵情報送付は、入出力制御部1301および処理選択部1302を経由して検証用公開鍵情報送付処理部1304に送られ、そこで処理される。

【0277】

図15は、本実施例のプロバイダが持つ検証用公開情報送付処理部1304の動作を示すフローチャートである。検証用公開情報送付処理部1304の動作を図15にしたがって説明する。

【0278】

まず、処理選択部1302から入力された検証用公開情報送付、および、該検証用公開情報送付に含まれる検証用公開鍵情報のデジタル署名を検証する（1501）。検証鍵は検証用公開情報送付の証明証フィールドに添付されているもの

を使用するが、必要な公開鍵証明書が証明書フィールドに存在しない場合には、CA111から公開鍵証明書を取得してから署名の検証を行う。署名の検証のために、検証用公開情報送付処理部1304はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【0279】

1501で、デジタル署名の検証に失敗した場合、エラー処理を行った後（1505）、終了する。

【0280】

1501で、デジタル署名の検証に成功した場合、検証用公開情報送付に含まれている検証用公開鍵情報の発行者がセンタであるかどうか調べられる（1502）。この検査は、検証用公開鍵情報の発行者フィールドに記載されている識別子がセンタのものであるかどうかで検査できる。

【0281】

1502の検査で、検証用公開鍵情報の発行者がセンタでなかった場合、エラー処理を行った後（1505）、終了する。

【0282】

1502の検査で、検証用公開鍵情報の発行者がセンタであったら、次に検証用公開鍵DB1306に新しいエントリを追加する（1503）。新しいエントリの各属性には以下の値が設定される。

【0283】

【表29】

公開鍵識別子属性：検証用公開情報送付に含まれている検証用公開鍵情報の検証用公開鍵識別子フィールドの値。

法数属性：検証用公開情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたRSA法数。

公開鍵属性：検証用公開情報送付に含まれている検証用公開鍵情報の、公開鍵情報フィールドに含まれていたRSA公開鍵。

有効期間開始属性：検証用公開情報送付に含まれている検証用公開鍵情報の有効期間開始日時フィールドの値。

有効期間終了属性：検証用公開情報送付に含まれている検証用公開鍵情報の有効期間終了日時フィールドの値。

用途属性：この検証用公開鍵にプロバイダが割り当てた用途についての情報。

【0284】

[予約証明証仲介許諾依頼処理部]

図16は、本実施例のプロバイダが持つ予約証明証仲介許諾依頼処理部1305の内部構成を示した図である。

【0285】

予約証明証仲介許諾依頼処理部1305は、予約証明証仲介許諾依頼を処理する機能を持ち、処理制御部1601、署名検証部1602、予約証明証仲介許諾識別子作成部1603、エラーメッセージ作成部1604、予約証明証仲介許諾作成部1605、予約証明証仲介許諾送付作成部1606、署名作成部1607、予約条件限定情報作成部1608から構成される。

【0286】

予約証明証仲介許諾依頼処理部1305を構成する各部の役割を以下に述べる。

【0287】

処理制御部1601：処理選択部1302からの入力、入出力制御部1301への出力、検証用公開鍵DB1306の参照、予約証明証仲介許諾発行履歴DB1309へのエントリの追加の機能を担うとともに、予約証明証仲介許諾依頼の処理全体を制御する。

署名検証部1602：処理選択部202から入力される予約証明証仲介許諾依頼のデジタル署名を検証する。

予約証明証仲介許諾識別子作成部1603：予約証明証仲介許諾に割り当てられる予約証明証仲介許諾識別子を作成する。十分に大きな空間からランダムにビット列を取り出す等、生成される識別子が重複しない工夫がなされている。

エラーメッセージ作成部1604：エラーメッセージを作成する。

予約証明証仲介許諾作成部1605：予約証明証仲介許諾を作成する。予約証明証仲介許諾にデジタル署名を添付するために署名作成部1607を呼び出す。

予約証明証仲介許諾送付作成部 1606：予約証明証仲介許諾送付を作成する。
予約証明証仲介許諾送付にデジタル署名を添付するために署名作成部 1607を呼び出す。さらに、プロバイダの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 1308にアクセスする。

署名作成部 1607：予約証明証仲介許諾、予約証明証仲介許諾送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 1307にアクセスする。

予約条件限定情報作成部 1608：予約証明証仲介許諾に記載される予約条件限定情報を作成する。

【0288】

図 17 は、本実施例のプロバイダが持つ予約証明証仲介許諾依頼処理部 1305の処理制御部 1601の動作を示すフローチャートである。処理制御部 1601の動作を図 17 にしたがって説明する。

【0289】

まず、処理選択部 1302から入力された予約証明証仲介許諾依頼のデジタル署名を検証する（1701）。検証鍵は予約証明証仲介許諾依頼の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA111から公開鍵証明証を取得してから署名の検証を行う。

【0290】

署名の検証に失敗した場合、エラーメッセージ作成部 1604でエラーメッセージを作成して入出力制御部 1301に出力した後（1709）、終了する。

【0291】

署名の検証に成功した場合、予約証明証仲介許諾依頼で依頼された予約証明証仲介許諾を発行するかどうかを決定する（1702）。予約証明証仲介許諾を発行するかどうかの決定はプロバイダにまかされている。例えば、予約証明証仲介許諾によって許諾を受けるリテラを信用できない場合や、予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の許諾者フィールドに記載されている識別子が自分のものと異なる場合や、予約証明証仲介許諾依頼に含まれる予約証明

証仲介許諾仕様の公開鍵識別子フィールドに記載された検証用公開鍵識別子を持つ検証用公開鍵情報が自分に対して発行されたものでない場合や、予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の希望予約条件限定情報フィールドの希望にそえない場合に予約証明証仲介許諾の発行をやめることになる。

【0292】

1702で、予約証明証仲介許諾を発行しないと決定した場合には、エラーメッセージ作成部1604でエラーメッセージを作成して入出力制御部1301に出力した後(1709)、終了する。

【0293】

1702で、予約証明証仲介許諾を発行すると決定した場合には、予約証明証仲介許諾識別子作成部1603を呼び出して予約証明証仲介許諾に割り当てる識別子を作成させ、作成された識別子を受け取った後(1703)、発行する予約証明証仲介許諾の有効期間を適切に決定する(1704)。

【0294】

さらに、予約条件限定情報作成部1608を呼び出して発行する予約証明証仲介許諾に含まれる予約条件限定情報を作成させ、その結果を受け取る(1705)。ここで作成する予約条件限定情報は、予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の希望予約条件限定情報フィールドに記載されているものでもよいし、プロバイダが自己の判断で適切な予約条件限定情報を決定してもよい。

【0295】

次に、予約証明証仲介許諾作成部1605を呼び出し、予約証明証仲介許諾を作成させ、その結果を受け取る(1706)。予約証明証仲介許諾の各フィールドには以下の値が設定される。

【0296】

【表30】

発行者フィールド：自分自身すなわちプロバイダの識別子。

受領者フィールド：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の被許諾者フィールドの値。

発行日フィールド：現在の日時。

予約証明証仲介許諾識別子フィールド：1703で作成した識別子。

有効期間開始日時フィールド：1704で決定した有効期間の開始日時。

有効期間終了日時フィールド：1704で決定した有効期間の終了日時。

公開鍵識別子フィールド：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の公開鍵識別子フィールドの値。

予約条件限定情報フィールド：1705で決定した予約条件限定情報の値。

デジタル署名フィールド：このフィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1607を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

【0297】

次に、予約証明証仲介許諾送付作成部1606を呼び出し、予約証明証仲介許諾送付を作成させ、その結果を受け取って入出力制御部1301に出力する（1707）。予約証明証仲介許諾送付の各フィールドには以下の値が設定される。

【0298】

【表31】

発信者フィールド：自分自身すなわちプロバイダの識別子。

受信者フィールド：予約証明証仲介許諾依頼の発信者フィールドに記載されている識別子。

日時フィールド：現在の日時。

予約証明証仲介許諾フィールド：1706で作成した予約証明証仲介許諾。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部1607を呼び出し、結果の署名値をこのフィールドに設定する。

証明証フィールド：証明証記憶部1308に記憶している公開鍵証明証。

【0299】

最後に予約証明証仲介許諾発行の履歴を表す新しいエントリを予約証明証仲介許諾発行履歴DB1309に追加して終了する。追加されるエントリの各属性には以下の値が格納される。

【0300】

【表32】

予約証明証仲介許諾識別子属性：1703で作成した識別子。

公開鍵識別子属性：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の公開鍵識別子フィールドの値。

リテラ識別子属性：予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の被許諾者フィールドの値。

予約条件限定情報属性：1705で決定した予約条件限定情報の値。

有効期間開始属性：1704で決定した有効期間の開始日時。

有効期間終了属性：1704で決定した有効期間の終了日時。

発行日属性：1706で作成した予約証明証仲介許諾の発行日フィールドに記載した値。

【0301】

[プロバイダが持つその他の機能]

本実施例のプロバイダは、予約証明証仲介許諾発行の履歴情報をリテラに送付する事ができる。

【0302】

リテラに渡される予約証明証仲介許諾発行の履歴情報は、そのリテラに発行された予約証明証仲介許諾についての情報であり、予約証明証仲介許諾発行履歴作成部1310で作成され、入出力制御部1301を介してリテラに送付される。この履歴は、プロバイダがリテラに対して予約証明証仲介許諾発行の手数料を請求する場合の根拠となる。

【0303】

予約証明証仲介許諾発行履歴作成部1310は、履歴を作成するリテラの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証仲介許諾発行履歴DB1309から、リテラ識別子属性の値が指定されたりテラの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その予約証明証仲介許諾識別子属性、公開鍵識別子属性、予約条件限定情報属性、有効期間開始属性、有効期間終了属性、発行日属性の値

を取り出す。本実施例では、履歴を作成するリテーラの識別子と履歴作成の対象期間の指定はプロバイダのオペレータから受けるが、インターネット経由でリテーラから入力されるように構成してもよい。

【0304】

上記の履歴情報の送付方法は、電子メールでもよいし、WWWベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【0305】

[リテーラの構成]

図18は、本実施例のリテーラの構成図である。

【0306】

本実施例のリテーラは、予約証明証仲介許諾依頼を作成してインターネットを介してプロバイダに送付する機能、インターネットを介して入力される予約証明証仲介許諾送付、予約証明証依頼、予約証明証送付を処理する機能、予約証明証仲介の履歴を作成してインターネットを介してプロバイダや予約証明証仲介の依頼者に送付する機能を持つ。リテーラは、入出力制御部1801、処理選択部1802、予約証明証仲介許諾依頼作成部1803、予約証明証依頼処理部1804、予約証明証仲介許諾送付処理部1805、予約証明証送付処理部1806、予約証明証仲介許諾DB1807、予約証明証仲介履歴DB1808、署名鍵記憶部1809、証明証記憶部1810、予約証明証仲介プロバイダ用履歴作成部1811、予約証明証仲介依頼者用履歴作成部1812から構成され、入出力制御部1801を介してインターネットに接続されている。

【0307】

本実施例のリテーラの各部の役割を以下に述べる。

【0308】

入出力制御部1801：インターネットを介したデータの入力を監視するとともに、予約証明証仲介許諾依頼作成部1803、予約証明証依頼処理部1804、予約証明証送付処理部1806が作成したデータをインターネットを介して出力する。インターネットからの入出力制御部1804への入力、あるいは、入出力

制御部1804からインターネットへの出力の方法としては、入出力制御部1804と接続されたWWWサイトを準備して他のエンティティにアクセスさせるもの、他のエンティティが用意しているWWWサイトにアクセスしてリテラが作成したデータを送るもの、あるいは電子メールシステムと入出力制御部1804を自動的にあるいは人手によって連動させるものなどが使用できる。

処理選択部1802：入力したデータが、予約証明証依頼、予約証明証仲介許諾送付、予約証明証送付のいずれであるかを判断し、予約証明証依頼であれば予約証明証依頼処理部1804を、予約証明証仲介許諾送付であれば予約証明証仲介許諾送付処理部1805を、予約証明証送付であれば予約証明証送付処理部1806を呼び出す。

予約証明証仲介許諾依頼作成部1803：予約証明証仲介許諾依頼を作成し、入出力制御部1801を介してプロバイダに送付する。予約証明証仲介許諾依頼作成の過程で、署名鍵記憶部1809と証明証記憶部1810にアクセスする。

予約証明証依頼処理部1804：消費者からの予約証明証依頼を処理し、第二の予約証明証依頼を作成して、入出力制御部1801を介してセンタに送付する。

処理の過程で、予約証明証仲介許諾DB1807を参照するとともに、予約証明証仲介履歴DB1808に新しいエントリを追加する。さらに、署名鍵記憶部1809と証明証記憶部1810にアクセスする。

予約証明証仲介許諾送付処理部1805：プロバイダからの予約証明証仲介許諾送付を処理し、該予約証明証仲介許諾送付に含まれている予約証明証仲介許諾を予約証明証仲介許諾DB1807に登録する。

予約証明証送付処理部1806：センタから送付された予約証明証送付を処理し、第二の予約証明証送付を作成して、入出力制御部1801を介して消費者に送付する。処理の過程で、予約証明証仲介履歴DB1808のエントリを更新するとともに、署名鍵記憶部1809と証明証記憶部1810にアクセスする。

予約証明証仲介許諾DB1807：プロバイダからこのリテラに対して発行された予約証明証仲介許諾を保持するDB。

予約証明証仲介履歴DB1808：このリテラが仲介した予約証明証についての履歴を保持するDB。

署名鍵記憶部 1809：リテラが作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部 1810：署名鍵記憶部 1809に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

予約証明証仲介プロバイダ用履歴作成部 1811：各プロバイダ毎の予約証明証仲介の履歴を作成し、入出力制御部 1801を介してプロバイダに送付する。

予約証明証仲介依頼者用履歴作成部 1812：リテラが受け取った予約証明証仲介依頼の依頼者毎の予約証明証仲介の履歴を作成し、入出力制御部 1801を介して依頼者に送付する。

【0309】

【リテラが持つデータベース】

リテラは、予約証明証仲介許諾DB 1807と予約証明証仲介履歴DB 1808の2つのデータベースを持っている。

【0310】

予約証明証仲介許諾DB 1807は、リテラが複数のプロバイダから受けた予約証明証仲介許諾に関する情報を保持したデータベースである。

【0311】

予約証明証仲介許諾DB 1807の構造を図19に示す。予約証明証仲介許諾DB 1807は以下の5つの属性からなるテーブルである。各エントリがそれぞれ一つの予約証明証仲介許諾にあたる。

【0312】

【表33】

予約証明証仲介許諾識別子属性：プロバイダから発行された予約証明証仲介許諾に割り当てられている予約証明証仲介許諾識別子。

公開鍵識別子属性：プロバイダから発行された予約証明証仲介許諾で予約証明証依頼の仲介が許諾された検証用公開鍵の識別子。

プロバイダ識別子属性：予約証明証仲介許諾を発行したプロバイダの識別子。

予約証明証仲介許諾属性：プロバイダから発行された予約証明証仲介許諾自体をBERにしたがってエンコードしたデータ。

プロバイダ証明証属性：予約証明証仲介許諾を発行したプロバイダのデジタル署名を検証できる公開鍵を含む公開鍵証明証をBERにしたがってエンコードしたデータ。

【0313】

予約証明証仲介履歴DB1808は、リテーラが仲介した予約証明証に関する情報を保持したデータベースである。

【0314】

予約証明証仲介履歴DB1808の構造を図20に示す。予約証明証仲介履歴DB1808は以下の8つの属性からなるテーブルである。各エントリがそれぞれ一つの予約証明証の仲介にあたる。

【0315】

【表34】

予約証明証識別子属性：仲介した予約証明証にセンタが割り当てた識別子。

公開鍵識別子属性：仲介した予約証明証の正当性を検証できる検証用公開鍵にセンタが割り当てた識別子。

プロバイダ識別子属性：公開鍵識別子属性で指定された検証用公開鍵情報のユーザであるプロバイダの識別子。

消費者識別子属性：予約証明証の発行を受けた消費者の識別子。

依頼者識別子属性：予約証明証依頼をリテーラに送付してきたエンティティの識別子。

予約条件属性：仲介された予約証明証に記載された予約条件。

依頼日時属性：リテーラが受け取った予約証明証依頼の作成日時。

発信日時属性：リテーラが予約証明証送付を作成した日時。

【0316】

[予約証明証仲介許諾依頼作成部]

本実施例のリテーラは、プロバイダが提供している物品やサービスの予約販売を始めたい場合、その物品やサービスに割りあてられた検証用公開鍵に対応する予約証明証の仲介を許諾する予約証明証仲介許諾をプロバイダから受けなければならない。プロバイダから予約証明証仲介許諾を受け取るため、リテーラは予約

証明証仲介許諾依頼作成部 1803 において予約証明証仲介許諾依頼を作成し、入出力制御部 1801 を介してプロバイダに送付する。

【0317】

予約証明証仲介許諾依頼作成部 1803 では、予約証明証仲介許諾依頼の各フィールドに以下の値を設定する。

【0318】

【表35】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：予約証明証仲介許諾の依頼先であるプロバイダの識別子。

日時フィールド：現在の時刻。

予約証明証仲介許諾仕様フィールド：作成してもらう予約証明証仲介許諾に対するリテーラからの希望を記載する。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、予約証明証仲介許諾依頼作成部 1803 は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部 1809 にアクセスして入手する。

証明証フィールド：証明証記憶部 1810 に記憶している公開鍵証明証。

予約証明証仲介許諾依頼の予約証明証仲介許諾仕様フィールドに記載される予約証明証仲介許諾仕様の各フィールドには以下の値が設定される。

許諾者フィールド：予約証明証仲介許諾を発行してほしいプロバイダの識別子。

被許諾者フィールド：自分自身すなわちリテーラの識別子。

公開鍵識別子フィールド：予約証明証仲介許諾を発行してほしい検証用公開鍵に割り当てられた検証用公開鍵識別子。

希望予約条件限定情報フィールド：リテーラが予約証明証仲介許諾に記載してほしいと希望する予約条件限定情報。

【0319】

[予約証明証仲介許諾送付処理部]

予約証明証仲介許諾依頼作成部 1803 で予約証明証仲介許諾依頼が作成され

プロバイダに送付されると、その返信としてプロバイダから予約証明証仲介許諾送付が送信されてくる。予約証明証仲介許諾送付は、入出力制御部1801および処理選択部1802を経由して予約証明証仲介許諾送付処理部1805に送られ、そこで処理される。

【0320】

図21は、本実施例のリテラが持つ予約証明証仲介許諾送付処理部1805の動作を示すフローチャートである。予約証明証仲介許諾送付処理部1805の動作を図21にしたがって説明する。

【0321】

まず、処理選択部1802から入力された予約証明証仲介許諾送付、および、該予約証明証仲介許諾送付に含まれる予約証明証仲介許諾のデジタル署名を検証する(2101)。検証鍵は予約証明証仲介許諾送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA111から公開鍵証明証を取得してから署名の検証を行う。署名の検証のために、予約証明証仲介許諾送付処理部1805はデジタル署名の検証を専門に行う署名検証部を含んでいる。

【0322】

2101で、デジタル署名の検証に失敗した場合、エラー処理を行った後(2104)、終了する。

【0323】

2101で、デジタル署名の検証に成功した場合、予約証明証仲介許諾送付に含まれている予約証明証仲介許諾の作成者が正しいプロバイダであるかどうかを確認される(2102)。正しいプロバイダであるかどうかの判断基準にはいくつかバリエーションが有り得る。たとえば、予約証明証仲介許諾送付に含まれている予約証明証仲介許諾の発行者フィールドの値が、自分が依頼した予約証明証仲介許諾依頼に含まれる予約証明証仲介許諾仕様の許諾者フィールドに記載されている識別子と一致するという基準はその一例である。予約証明証仲介許諾送付に含まれている予約証明証仲介許諾で予約証明証の仲介が許諾される検証用公開鍵と、該予約証明証仲介許諾の発行者との関係を確認したければ、センタが発行

した検証用公開鍵情報を確認すればよい。検証用公開鍵情報は公開可能な情報であるので、センタあるいはプロバイダが検証用公開鍵情報を自由にダウンロードできる形で公開することが可能である。

【0324】

2102の検査で、予約証明証仲介許諾の作成者が正しいプロバイダではなかった場合、エラー処理を行った後（2104）、終了する。

【0325】

2102の検査で、予約証明証仲介許諾の作成者が正しいプロバイダであると判断した場合、予約証明証仲介許諾DB1807に新しいエントリを追加する（2103）。新しいエントリの各属性には以下の値が設定される。

【0326】

【表36】

予約証明証仲介許諾識別子属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾の予約証明証仲介許諾識別子フィールドの値。

公開鍵識別子属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾の公開鍵識別子フィールドの値。

プロバイダ識別子属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾の発行者フィールドの値。

予約証明証仲介許諾属性：予約証明証仲介許諾送付に含まれる予約証明証仲介許諾をBERにしたがってエンコードした結果。

プロバイダ証明証属性：予約証明証仲介許諾送付に含まれるプロバイダの署名の検証鍵を含む公開鍵証明証をBERにしたがってエンコードした結果。

【0327】

【予約証明証依頼処理部】

図22は、本実施例のリテーラが持つ予約証明証依頼処理部1804の内部構成を示した図である。

【0328】

予約証明証依頼処理部1804は、消費者あるいは他のリテーラから送信された予約証明証依頼を処理し、センタへの予約証明証依頼を作成し、入出力制御部

1801 経由でセンタへ送付する機能を持ち、処理制御部 2201、署名検証部 2202、エラーメッセージ作成部 2203、予約証明証依頼作成部 2204、署名作成部 2205、予約条件作成部 2206 から構成される。

【0329】

予約証明証依頼処理部 1804 を構成する各部の役割を以下に述べる。

【0330】

処理制御部 2201：処理選択部 1802 からの入力、入出力制御部 1801 への出力、予約証明証仲介許諾 DB 1807 の参照、予約証明証仲介履歴 DB 1808 へのエントリの追加の機能を担うとともに、予約証明証依頼の処理全体を制御する。

署名検証部 2202：処理選択部 1802 から入力される予約証明証依頼のデジタル署名を検証する。

エラーメッセージ作成部 2203：エラーメッセージを作成する。

予約証明証依頼作成部 2204：センタへ送付する予約証明証依頼を作成する。予約証明証依頼にデジタル署名を添付するために署名作成部 2205 を呼び出す。さらに、リテラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部 1810 にアクセスする。

署名作成部 2205：予約証明証依頼作成部 2204 で作成する予約証明証依頼のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部 1809 にアクセスする。

予約条件作成部 2206：依頼する予約証明証に含まれるべき予約条件を作成する。

【0331】

図 23 は、本実施例のリテラが持つ予約証明証依頼処理部 1804 の処理制御部 2201 の動作を示すフローチャートである。処理制御部 2201 の動作を図 23 にしたがって説明する。

【0332】

まず、処理選択部 1802 から入力された予約証明証依頼のデジタル署名を検証する（2301）。検証鍵は該予約証明証依頼の証明証フィールドに添付され

ているものを使用するが、必要な公開鍵証明書が証明書フィールドに存在しない場合には、CA111から公開鍵証明書を取得してから署名の検証を行う。

【0333】

署名の検証に失敗した場合、エラーメッセージ作成部2203でエラーメッセージを作成して入出力制御部1801に出力した後(2307)、終了する。

【0334】

署名の検証に成功した場合、入力された予約証明書依頼で予約証明書の仲介を依頼されている検証用公開鍵の仲介が許諾されているかどうかを検査する(2302)。予約証明書仲介許諾DB1807に、予約証明書依頼で依頼された検証用公開鍵に対する予約証明書仲介許諾が存在し、かつ予約証明書依頼に記載されている予約条件が、予約証明書仲介許諾DB1807に保持されている予約証明書仲介許諾に記載されている予約条件限定情報の範囲内である場合に許諾されていると判断する。

【0335】

2302の検査で仲介が許諾されていないと判断された場合、エラーメッセージ作成部2203でエラーメッセージを作成して入出力制御部1801に出力した後(2307)、終了する。

【0336】

2302の検査で仲介が許諾されていると判断された場合、予約証明書依頼を受け付けるかどうかを判断する(2303)。入力された予約証明書依頼の発信者である消費者やリテラが信用できない場合は、ここで予約証明書依頼を受け付けないことを決定する。

【0337】

2303で予約証明書依頼を受け付けないと判断した場合、エラーメッセージ作成部2203でエラーメッセージを作成して入出力制御部1801に出力した後(2307)、終了する。

【0338】

2303で予約証明書依頼を受け付けると判断した場合、予約条件作成部2206を呼び出し、センタへ送付する予約証明書依頼に記載する予約条件を作成さ

せ、その結果を受けとる（2304）。予約条件作成部2206が作成する予約条件は、入力された予約証明証依頼に記載されている予約条件のままでもよいし、必要ならリテラの裁量で適切なものに修正してもよい。

【0339】

予約条件が決まったら、処理中の予約証明証依頼に関する情報を保持したエントリを予約証明証仲介履歴DB1808に追加する（2305）。新しいエントリの各属性には以下の値が設定される。

【0340】

【表37】

予約証明証識別子属性：この時点では値は設定されない。

公開鍵識別子属性：入力された予約証明証依頼に含まれる予約仕様の公開鍵識別子フィールドに記載されている値。

プロバイダ識別子属性：公開鍵識別子属性に設定された識別子で特定される検証用公開鍵情報のユーザであるプロバイダの識別子。該プロバイダの識別子は、予約証明証仲介許諾DBを参照して得ることができる。すなわち、本DBの公開鍵識別子属性に設定された識別子を予約証明証仲介許諾DBの公開鍵識別子属性の値に持つ予約証明証仲介許諾DBのエントリのプロバイダ識別子属性がそれにあたる。

消費者識別子属性：入力された予約証明証依頼に含まれる予約仕様の消費者識別子フィールドの値。

依頼者識別子属性：入力された予約証明証依頼の発信者フィールドの値。

予約条件属性：2304で決定した予約条件。

依頼日時属性：入力された予約証明証依頼の日時フィールドの値。

発信日時属性：この時点では値は設定されない。

【0341】

最後にセンタへ送付する予約証明証依頼を作成し、入出力制御部1801を介してセンタに送付し（2306）、終了する。センタへ送付する予約証明証依頼の各フィールドには以下の値が設定される。

【0342】

【表 3 8】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：センタの識別子。

日時フィールド：現在の日時。

予約内容フィールド：後述する予約仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部 2205 を呼び出して署名値を作成させ、結果をこのフィールドに設定する。署名鍵は署名鍵記憶部 1809 にアクセスして入手する。

証明証フィールド：証明証記憶部 1810 に記憶している公開鍵証明証。

【0343】

予約内容フィールドに記載される予約仕様の各フィールドには、以下の値が記載される。

【0344】

【表 3 9】

公開鍵識別子フィールド：入力された予約証明証依頼に含まれる予約仕様の公開鍵識別子フィールドに記載されている値。

消費者識別子フィールド：入力された予約証明証依頼に含まれる予約仕様の消費者識別子フィールドに記載されている値。

予約条件フィールド：2304 で決定した予約条件。

予約証明証仲介許諾フィールド：予約証明証仲介許諾 DB 1807 に保持されている、予約証明証依頼で予約証明証の発行を依頼された検証用公開鍵に対する予約証明証仲介許諾。

【0345】

【予約証明証送付処理部】

図 24 は、本実施例のリテーラが持つ予約証明証送付処理部 1806 の内部構成を示した図である。

【0346】

予約証明証送付処理部 1806 は、センタあるいは他のリテーラからの送信さ

れた予約証明証送付を処理し、予約証明証の依頼者に送付する予約証明証送付を作成し、入出力制御部1801経由で該依頼者に送付する機能を持ち、処理制御部2401、署名検証部2402、エラーメッセージ作成部2403、予約証明証送付作成部2404、署名作成部2405から構成される。

【0347】

予約証明証送付処理部1806を構成する各部の役割を以下に述べる。

【0348】

処理制御部2401：処理選択部1802からの入力、入出力制御部1801への出力、予約証明証仲介履歴DB1808のエントリ更新の機能を担うとともに、予約証明証送付の処理全体を制御する。

署名検証部2402：処理選択部1802から入力される予約証明証送付、および予約証明証送付に含まれる予約証明証のデジタル署名を検証する。

エラーメッセージ作成部2403：エラーメッセージを作成する。

予約証明証送付作成部2404：予約証明証の依頼者に送付する予約証明証送付を作成する。新たに作成する予約証明証送付にデジタル署名を添付するために署名作成部2405を呼び出す。さらに、リテラの署名の検証鍵の公開鍵証明証を入手するために証明証記憶部1810にアクセスする。

署名作成部2405：予約証明証送付作成部2404で作成する予約証明証送付のためのデジタル署名を作成する。デジタル署名のための署名鍵を入手するために、署名鍵記憶部1809にアクセスする。

【0349】

図25は、本実施例のリテラが持つ予約証明証送付処理部1806の処理制御部2401の動作を示すフローチャートである。処理制御部2401の動作を図25にしたがって説明する。

【0350】

まず、処理選択部1802から入力された予約証明証送付および該予約証明証送付に含まれる予約証明証のデジタル署名を検証する(2501)。検証鍵は該予約証明証送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA111から公開鍵

証明証を取得してから署名の検証を行う。

【0351】

署名の検証に失敗した場合、エラーメッセージ作成部2403でエラーメッセージを作成して入出力制御部1801に出力した後(2504)、終了する。

【0352】

署名の検証に成功した場合、入力された予約証明証送付で送付された内容にしたがって、予約証明証仲介履歴DB1808のエントリを更新する(2502)。更新されるエントリは、入力された予約証明証送付に対応する予約証明証依頼を処理した時に追加されたエントリであり、エントリの公開鍵識別子属性、消費者識別子属性の値が、それぞれ入力された予約証明証送付に含まれる予約証明証の公開鍵識別子フィールド、受領者フィールドの値と一致し、該エントリの予約証明証識別子属性と発信日時属性の値が設定されていないものである。

【0353】

更新対象のエントリの各属性は以下のように更新される。

【0354】

【表40】

予約証明証識別子属性：入力された予約証明証送付に含まれる予約証明証の予約証明証識別子フィールドの値。

公開鍵識別子属性：変化なし。

プロバイダ識別子属性：変化なし。

消費者識別子属性：変化なし。

依頼者識別子属性：変化なし。

予約条件属性：入力された予約証明証送付に含まれる予約証明証の予約条件フィールドの値。

依頼日時属性：変化なし。

発信日時属性：現在の時刻。

【0355】

最後に、予約証明証の依頼者に送付する新たな予約証明証送付を作成し、入出力制御部1801を介して予約証明証の依頼者に送付し(2503)、終了する。

。新たに作成される予約証明証送付の各フィールドには以下の値が設定される。

【0356】

【表41】

発信者フィールド：自分自身すなわちリテーラの識別子。

受信者フィールド：2502で更新された予約証明証仲介履歴DB1808のエントリの依頼者識別子属性の値。

日時フィールド：2502で更新された予約証明証仲介履歴DB1808のエントリの発信日時属性の値。

予約証明証フィールド：入力された予約証明証送付に含まれる予約証明証。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、署名作成部2405を呼び出し、結果の署名値を受け取り、このフィールドに設定する。

証明証フィールド：証明証記憶部1810に記憶している公開鍵証明証と、入力された予約証明証送付の証明証フィールドに含まれる証明証のうち、該予約証明証送付に含まれる予約証明証のデジタル署名を検証できる検証鍵を含む公開鍵証明証。

【0357】

〔予約証明証依頼処理の課金・決済〕

本実施例のリテーラは、予約証明証依頼の処理の過程で予約証明証発行料金の課金あるいは決済を行うことができる。課金あるいは決済の処理は、消費者からの予約証明証依頼をうけた後、センタに予約証明証依頼を送付する前に行われる。

【0358】

課金の場合は、予約証明証依頼の処理の過程で、消費者毎に予約証明証発行料金を加算しておき、後に消費者に対して請求する。そのため、本実施例のリテーラは、消費者毎に現在の予約証明証発行料金高を保持するデータベースをもっている。

【0359】

本実施例のリテーラは、予約証明証依頼の処理のたび毎に予約証明証発行料金

の決済を行うこともできる。決済の方法としては、消費者が所持するクレジットカードによる決済や、プリペイドの方式等種々のものが利用可能であるが、いずれも、消費者からの予約証明証依頼を受けた後、決済が終了した事が確認されてから、センタに予約証明証依頼を送付する。

【0360】

また、予約証明証発行料金を予約証明証の検証時にプロバイダに回収させる事もできる。

【0361】

この場合、予約証明証に含まれる予約条件に料金情報を記載しておき、プロバイダが設置している予約証明証検証機器が予約証明証を検証する際に、予約証明証に含まれる予約条件が満たされているかどうかの判定の際に、料金が人手あるいは自動的に徴収されたことを確認すればよい。

【0362】

〔リテーラが発行する履歴情報〕

本実施例のリテーラは予約証明証仲介の履歴情報をプロバイダに送付する事ができる。

【0363】

プロバイダに渡される予約証明証仲介の履歴情報は、そのプロバイダに割り当てられた検証用公開鍵に対応する予約証明証の仲介についての情報であり、予約証明証仲介プロバイダ用履歴作成部1811で作成され、入出力制御部1801を介してプロバイダに送付される。この履歴は、リテーラがプロバイダに送付するマージンの額に対する根拠となる。

【0364】

予約証明証仲介プロバイダ用履歴作成部1811は、履歴を作成するプロバイダの識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証仲介履歴DB1808から、プロバイダ識別子属性の値が指定されたプロバイダの識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その予約証明証識別子属性、公開鍵識別子属性、予約条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作

成するプロバイダの識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由でプロバイダから入力されるように構成してもよい。

【0365】

また、本実施例のリテーラは予約証明証仲介の履歴情報を予約証明証仲介の依頼者にも送付することができる。

【0366】

依頼者に渡される予約証明証仲介の履歴情報は、その依頼者から依頼された予約証明証の仲介についての情報であり、予約証明証仲介依頼者用履歴作成部1812で作成され、入出力制御部1801を介して依頼者に送付される。この履歴は、リテーラが依頼者に対して手数料の請求を行う場合の根拠となる。

【0367】

予約証明証仲介依頼者用履歴作成部1812は、履歴を作成する依頼者の識別子と履歴作成の対象期間の開始日時と終了日時の指定を受け、予約証明証仲介履歴DB1808から、依頼者識別子属性の値が指定された依頼者の識別子と一致し、発行日属性の値が指定された履歴作成の対象期間内であるエントリ群を取り出し、その予約証明証識別子属性、公開鍵識別子属性、プロバイダ識別子属性、消費者識別子属性、予約条件属性、依頼日時属性、発信日時属性の値を取り出す。本実施例では、履歴を作成する依頼者の識別子と履歴作成の対象期間の指定はリテーラのオペレータから受けるが、インターネット経由で依頼者から入力されるように構成してもよい。

【0368】

上記の履歴情報のプロバイダや依頼者への送付方法は、電子メールでもよいし、WWWベースでオンデマンドで発行してもよい。盗聴や改竄の危険がある場合は暗号化やデジタル署名が適用されるのが望ましい。

【0369】

[消費者端末の構成]

図26は、本実施例の消費者端末の構成図である。

【0370】

本実施例の消費者端末は、インターネットを介してリテーラから予約証明証を受け取る。予約証明証依頼を作成してインターネットを介してリテーラに送付する機能と、インターネットを介してリテーラから送付される予約証明証送付を処理する機能を持つ。消費者端末は、入出力制御部2602、予約証明証依頼作成部2603、予約証明証送付処理部2604、署名鍵記憶部2605、証明証記憶部2606、携帯型記憶装置制御部2607から構成され、入出力制御部2602を介してインターネットに接続されるとともに、携帯型記憶装置制御部2607を介して携帯型記憶装置と接続されている。

【0371】

本実施例の消費者端末の各部の役割を以下に述べる。

【0372】

入出力制御部2602：インターネットを介したデータの入力を受け付けるとともに、予約証明証依頼作成部2603が作成した予約証明証依頼をインターネットを介して出力する。インターネットからの入出力制御部2602への入力、あるいは、入出力制御部2602からインターネットへの出力の方法としては、他のエンティティが用意しているWWWサイトにアクセスして消費者端末が作成したデータを送るもの、あるいは電子メールシステムと入出力制御部2602を自動的にあるいは人手によって連動させるものなどが使用できる。

予約証明証依頼作成部2603：予約証明証依頼を作成し、入出力制御部2602を介してリテーラに送付する。予約証明証依頼の作成の過程で、署名鍵記憶部2605と証明証記憶部2606にアクセスするとともに、携帯型記憶装置制御部2607を介して携帯型記憶装置2608にアクセスする。

予約証明証送付処理部2604：リテーラからの予約証明証送付を処理し、該予約証明証送付に含まれている予約証明証を携帯型記憶装置制御部2607を介して携帯型記憶装置2608に記録する。

署名鍵記憶部2605：消費者端末が作成するデジタル署名に使用する署名鍵を保持する。

証明証記憶部2606：署名鍵記憶部2605に記憶されている署名鍵で作成したデジタル署名を検証できる検証鍵を含む公開鍵証明証を保持する。

携帯型記憶装置制御部 2607：携帯型記憶装置 2608 へのデータの書込みとアクセスを行う。

【0373】

本実施例では、予約証明証依頼にデジタル署名を施す場合に使用する署名鍵や、その署名鍵で作成した署名を検証する検証鍵を含む公開鍵証明証は、消費者端末が保持しているものとしたが、これらが携帯型記憶装置に保持されているように構成してもよい。

【0374】

[予約証明証依頼作成部]

本実施例の消費者端末は、該端末を利用している消費者が予約したい物品やサービスがある場合、その物品やサービスの予約証明証の仲介を依頼する予約証明証依頼を予約証明証依頼作成部 2603 で作成し、入出力制御部 2602 を介してリテーラに送付する。

【0375】

予約証明証依頼作成部 2603 では、予約証明証依頼の各フィールドに以下の値を設定する。

【0376】

【表 4 2】

発信者フィールド：自分自身すなわち消費者端末の識別子。

受信者フィールド：リテーラの識別子。

日時フィールド：現在の時刻。

予約内容フィールド：後述する予約仕様。

デジタル署名フィールド：このフィールドおよび証明証フィールド以外のフィールドのデータに対するデジタル署名。デジタル署名の作成のため、予約証明証依頼作成部 2603 は署名作成部を含んでおり、この署名作成部が作成した署名値をこのフィールドに設定する。署名鍵は署名鍵記憶部 2605 にアクセスして入手する。

証明証フィールド：証明証記憶部 2606 に記憶している公開鍵証明証。

予約内容フィールドに指定される予約仕様の各フィールドには以下の値が設定さ

れる。

公開鍵識別子フィールド：予約したい物品やサービスに割り当てられている検証用公開鍵の識別子。

消費者識別子フィールド：消費者端末を使用している消費者の識別子。消費者識別子は携帯型記憶装置2608に記憶されており、予約証明証依頼作成部2603は、携帯型記憶装置制御部2607を介して携帯型記憶装置2608から消費者識別子を入力する。

予約条件フィールド：消費者の希望等を反映した適切なものを予約証明証依頼作成部2603が決定して設定。

予約証明証仲介承諾フィールド：設定しない。

【0377】

[予約証明証送付処理部]

予約証明証依頼作成部2603で予約証明証依頼が作成されリテーラに送付されると、その返信としてリテーラから予約証明証送付が送信されてくる。予約証明証送付は、入出力制御部2602を経由して予約証明証送付処理部2604に入力され、そこで処理される。

【0378】

図27は、本実施例の消費者端末が持つ予約証明証送付処理部2604の動作を示すフローチャートである。予約証明証送付処理部2604の動作を図27にしたがって説明する。

【0379】

まず、入力された予約証明証送付および該予約証明証送付に含まれる予約証明証のデジタル署名を検証する(2701)。検証鍵は検証用公開情報送付の証明証フィールドに添付されているものを使用するが、必要な公開鍵証明証が証明証フィールドに存在しない場合には、CA111から公開鍵証明証を取得してから署名の検証を行う。

【0380】

2701で、デジタル署名の検証に失敗した場合、エラー処理を行った後(2704)、終了する。

【0381】

2701で、デジタル署名の検証に成功した場合、入力された予約証明証送付に含まれる予約証明証が、現在消費者端末を使用している消費者向けのものかどうかを検査される(2702)。検査は、携帯型記憶装置制御部2607を介して携帯型記憶装置2608から入手した消費者識別子と、入力された予約証明証送付に含まれる予約証明証の受領者フィールドの値が一致するかどうかで行われる。

【0382】

2702の検査で、入力された予約証明証送付に含まれる予約証明証が現在消費者端末を使用している消費者向けのものでないと判断された場合、エラー処理を行った後(2704)、終了する。

【0383】

2702の検査で、入力された予約証明証送付に含まれる予約証明証が現在消費者端末を使用している消費者向けのものであると判断された場合、該予約証明証を携帯型記憶装置制御部2607を介して携帯型記憶装置2608に記録し(2703)、終了する。

【0384】

【発明の効果】

以上説明したようにこの発明によれば予約販売を行う際に予約販売業者は証明証を発行するリソースを自ら構築する必要がない。

【図面の簡単な説明】

【図1】 本発明を適用した実施例の構成図である。

【図2】 本発明を適用したセンタの構成図である。

【図3】 本発明を適用したセンタの動作を示すフローチャートである。

【図4】 本発明を適用したセンタが持つ検証用公開情報依頼処理部の内部構成を示した図である。

【図5】 本発明を適用したセンタが持つ検証用公開情報依頼処理部の処理制御部の動作を示すフローチャートである。

【図6】 本発明を適用したセンタが持つプロバイダDBの構造を示した図で

ある。

【図 7】本発明を適用したセンタが持つ公開鍵ペア DB の構造を示した図である。

【図 8】本発明を適用したセンタが持つリテーラ DB の構造を示した図である。

【図 9】本発明を適用したセンタが持つ消費者 DB の構造を示した図である。

【図 10】本発明を適用したセンタが持つ予約証明証発行履歴 DB の構造を示した図である。

【図 11】本発明を適用したセンタが持つ予約証明証依頼処理部の内部構成を示した図である。

【図 12】本発明を適用したセンタが持つ予約証明証依頼処理部の処理制御部の動作を示すフローチャートである。

【図 13】本発明を適用したプロバイダの構成図である。

【図 14】本発明を適用したプロバイダが持つ検証用公開鍵 DB の構造を示した図である。

【図 15】本発明を適用したプロバイダが持つ検証用公開情報送付処理部の動作を示すフローチャートである。

【図 16】本発明を適用したプロバイダが持つ予約証明証仲介許諾依頼処理部の内部構成を示した図である。

【図 17】本発明を適用したプロバイダが持つ予約証明証仲介許諾依頼処理部の処理制御部の動作を示すフローチャートである。

【図 18】本発明を適用したリテーラの構成図である。

【図 19】本発明を適用したリテーラが持つ予約証明証仲介許諾 DB の構造を示した図である。

【図 20】本発明を適用したリテーラが持つ予約証明証仲介履歴 DB の構造を示した図である。

【図 21】本発明を適用したリテーラが持つ予約証明証仲介許諾送付処理部の動作を示すフローチャートである。

【図 2 2】本発明を適用したリテーラが持つ予約証明証依頼処理部の内部構成を示した図である。

【図 2 3】本発明を適用したリテーラが持つ予約証明証依頼処理部の処理制御部の動作を示すフローチャートである。

【図 2 4】本発明を適用したリテーラが持つ予約証明証送付処理部の内部構成を示した図である。

【図 2 5】本発明を適用したリテーラが持つ予約証明証送付処理部の処理制御部の動作を示すフローチャートである。

【図 2 6】本発明を適用した消費者端末の構成図である。

【図 2 7】本発明を適用した消費者端末が持つ予約証明証送付処理部の動作を示すフローチャートである。

【図 2 8】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第 1 の構成例を示した図である。

【図 2 9】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第 1 の構成例における、予約証明証の検証の際の予約証明証検証機器と携帯型記憶装置の動作を示すフローチャートである。

【図 3 0】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第 2 の構成例を示した図である。

【図 3 1】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第 2 の構成例における、予約証明証の検証の際の予約証明証検証機器と携帯型記憶装置の動作を示すフローチャートである。

【図 3 2】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第 3 の構成例を示した図である。

【図 3 3】消費者が保持する携帯型記憶装置と予約証明証の検証機器の第 3 の構成例における、予約証明証の検証の際の予約証明証検証機器と携帯型記憶装置の動作を示すフローチャートである。

【図 3 4】本発明を適用したプロバイダが持つ予約証明証仲介許諾発行履歴 DB の構造を示した図である。

【符号の説明】

- 101 インターネット
- 102 予約証明証発行センタ
- 103、104 リテラ
- 105、107 プロバイダ
- 106、108 検証機器
- 109 消費者端末
- 110 携帯型記憶装置
- 111 認証局 (Certificate Authority)
- 201 入出力制御部
- 202 処理選択部
- 203 検証用公開鍵情報依頼処理部
- 204 予約証明証依頼処理部
- 205 プロバイダDB
- 206 公開鍵ペアDB
- 207 リテラDB
- 208 消費者DB
- 209 予約証明証発行履歴DB
- 210 署名鍵記憶部
- 211 証明証記憶部
- 212 予約証明証発行プロバイダ用履歴作成部
- 213 予約証明証発行リテラ用履歴作成部
- 214 検証用公開鍵情報発行履歴作成部
- 401 処理制御部
- 402 署名検証部
- 403 公開鍵ペア作成部
- 404 公開鍵ペア識別子作成部
- 405 検証用公開鍵情報作成部
- 406 検証用公開鍵情報送付作成部
- 407 エラーメッセージ作成部

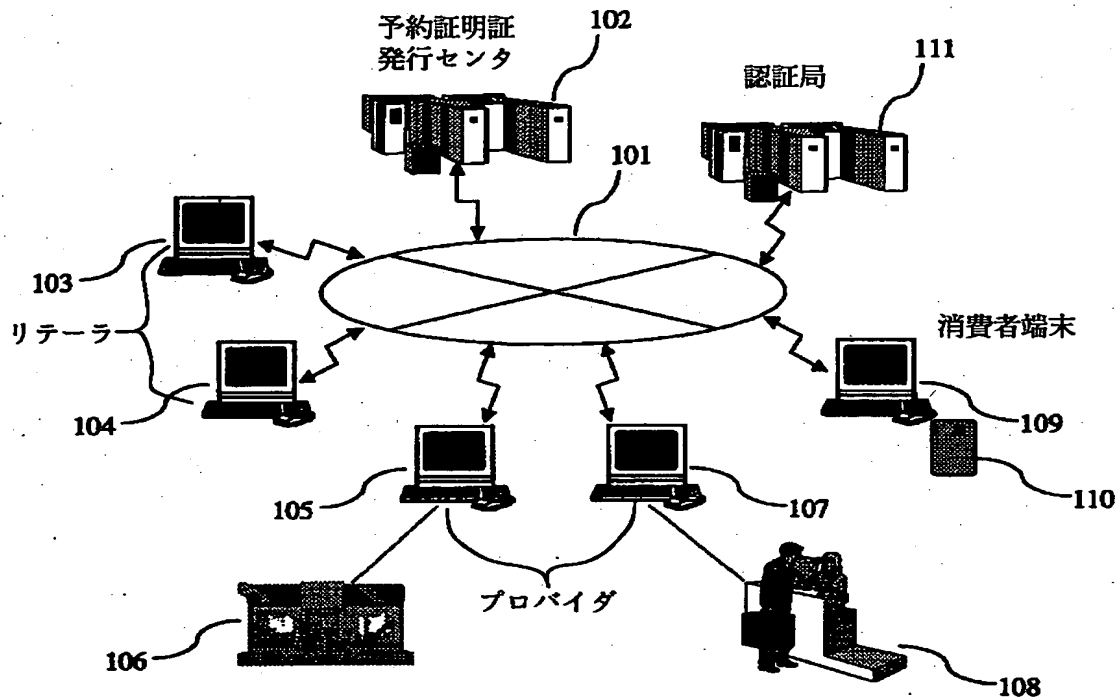
- 4 0 8 署名作成部
- 1 1 0 1 処理制御部
- 1 1 0 2 署名検証部
- 1 1 0 3 予約証明証仲介許諾内容確認部
- 1 1 0 4 予約証明証識別子作成部
- 1 1 0 5 予約証明証作成部
- 1 1 0 6 予約証明証送付作成部
- 1 1 0 7 エラーメッセージ作成部
- 1 1 0 8 署名作成部
- 1 1 0 9 予約値作成部
- 1 1 1 0 予約条件作成部
- 1 3 0 1 入出力制御部
- 1 3 0 2 処理選択部
- 1 3 0 3 検証用公開鍵情報依頼作成部
- 1 3 0 4 検証用公開鍵情報送付処理部
- 1 3 0 5 予約証明証仲介許諾依頼処理部
- 1 3 0 6 検証用公開鍵 D B
- 1 3 0 7 署名鍵記憶部
- 1 3 0 8 証明証記憶部
- 1 3 0 9 予約証明証仲介許諾発行履歴 D B
- 1 3 1 0 予約証明証仲介許諾発行履歴作成部
- 1 8 0 1 入出力制御部
- 1 8 0 2 処理選択部
- 1 8 0 3 予約証明証仲介許諾依頼作成部
- 1 8 0 4 予約証明証依頼処理部
- 1 8 0 5 予約証明証仲介許諾送付処理部
- 1 8 0 6 予約証明証送付処理部
- 1 8 0 7 予約証明証仲介許諾 D B
- 1 8 0 8 予約証明証仲介履歴 D B

1 8 0 9	署名鍵記憶部
1 8 1 0	証明証記憶部
1 8 1 1	予約証明証仲介プロバイダ用履歴作成部
1 8 1 2	予約証明証仲介依頼者用履歴作成部
2 6 0 1	消費者端末
2 6 0 2	入出力制御部
2 6 0 3	予約証明証依頼作成部
2 6 0 4	予約証明証送付処理部
2 6 0 5	署名鍵記憶部
2 6 0 6	証明証記憶部
2 6 0 7	携帯型記憶装置制御部
2 6 0 8	携帯型記憶装置
2 8 0 1	予約証明証検証機器
2 8 0 2	条件指定記憶部
2 8 0 3	チャレンジ生成部
2 8 0 4	公開鍵情報記憶部
2 8 0 5	レスポンス検査部
2 8 0 6	携帯型記憶装置制御部
2 8 1 1	携帯型記憶装置
2 8 1 2	入出力制御部
2 8 1 3	消費者秘密情報記憶部
2 8 1 4	レスポンス計算部
2 8 1 5	予約条件判定部
2 8 1 6	予約証明証記憶部

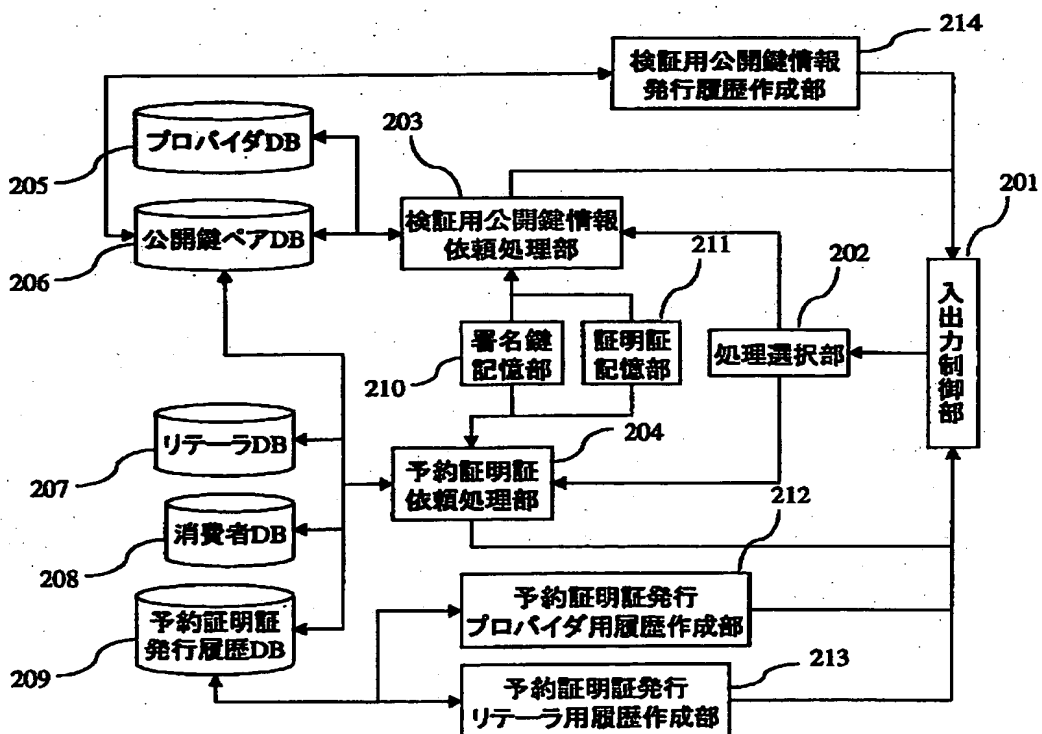
【書類名】

図面

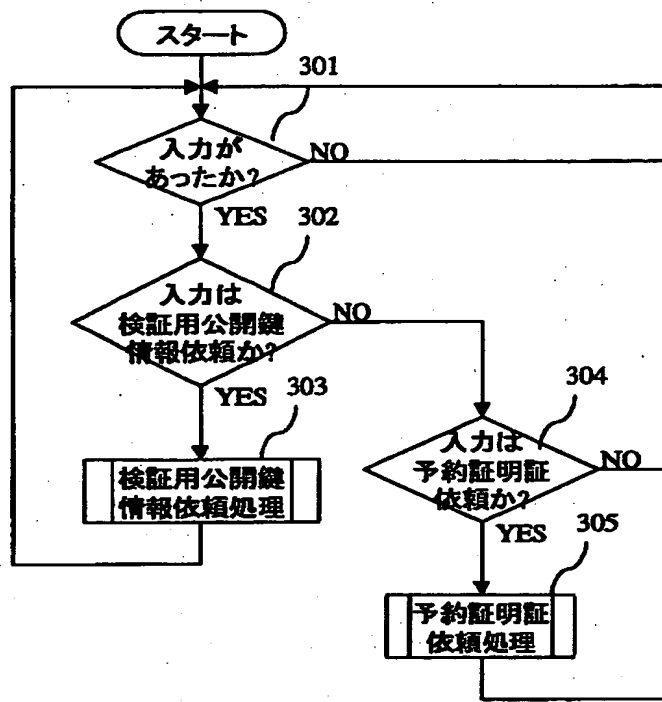
【図 1】



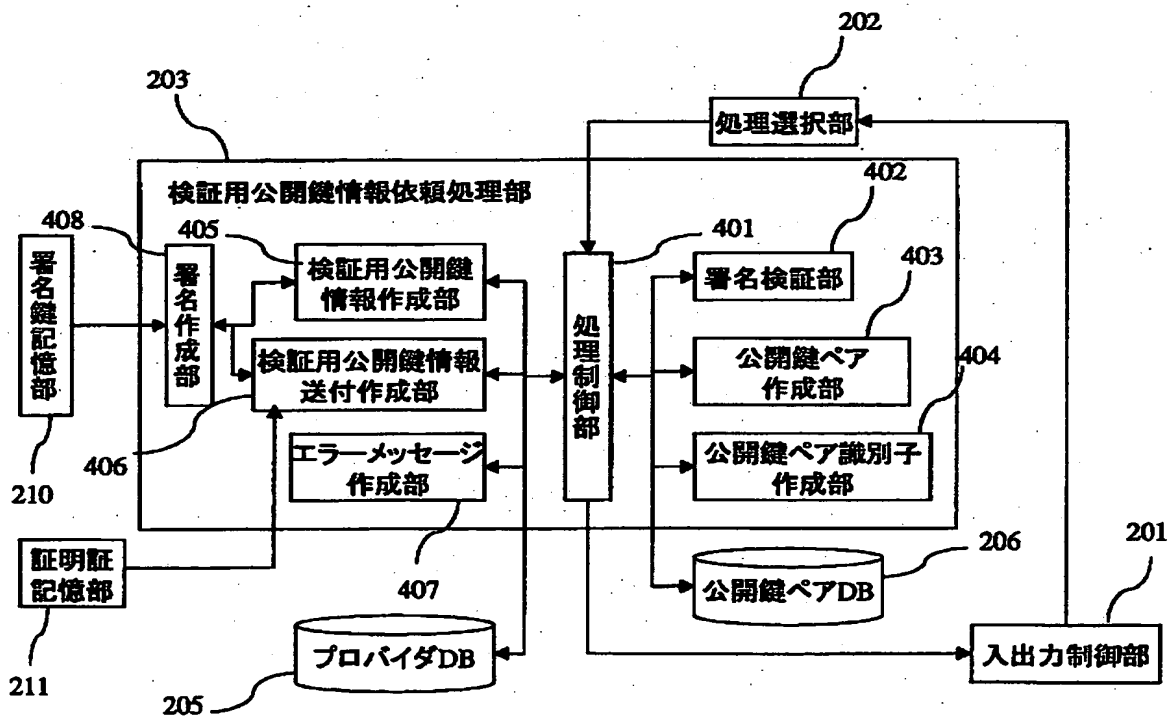
【図 2】



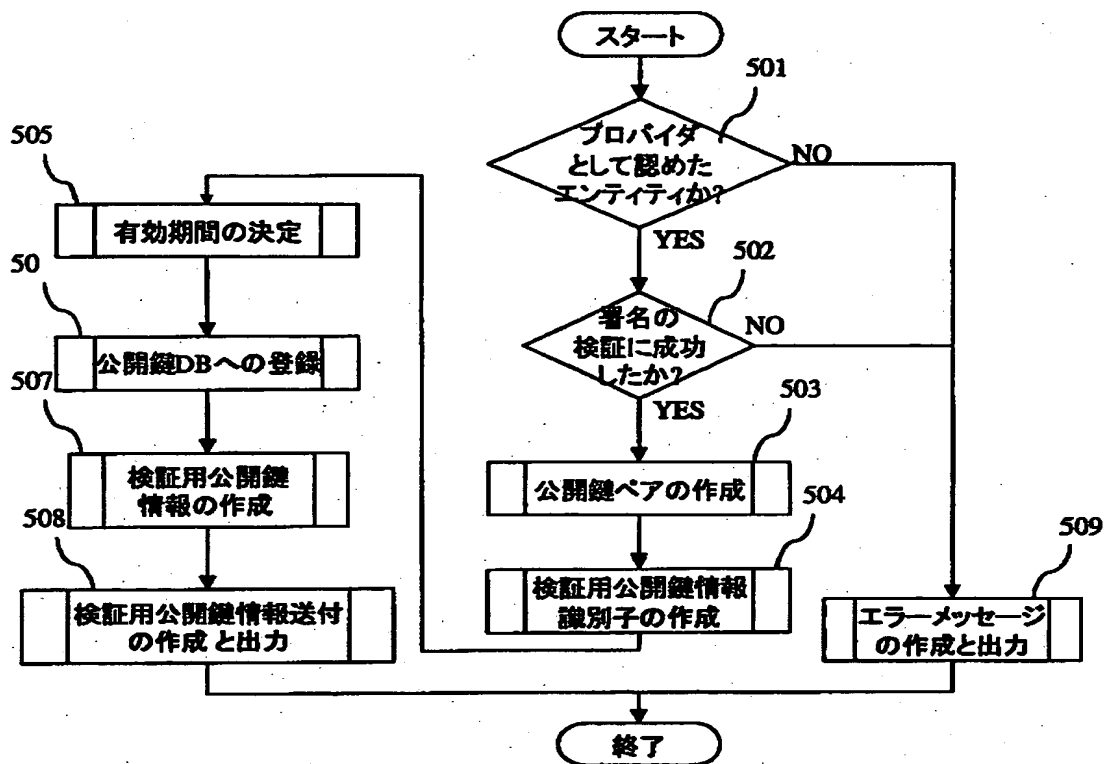
【図 3】



【図 4】



【図 5】



【図 6】

プロバイダ識別子
PRV10001
PRV10002
PRV10003
...

【図 7】

公開鍵識別子	法数	公開鍵	秘密鍵	プロバイダ識別子	有効期間開始	有効期間終了	発行日
PK00001	10110...	11001...	10101...	PRV10001	2000.1.1	2001.1.1	2000.12.1
PK00002	10010...	11110...	11011...	PRV10003	1999.3.5	2000.2.3	2000.1.2
PK00003	11111...	10000...	10101...	PRV10001	1999.11.1	2000.5.1	2000.3.1
...

【図 8】

リテラ識別子
RTL10001
RTL10002
RTL10003
...

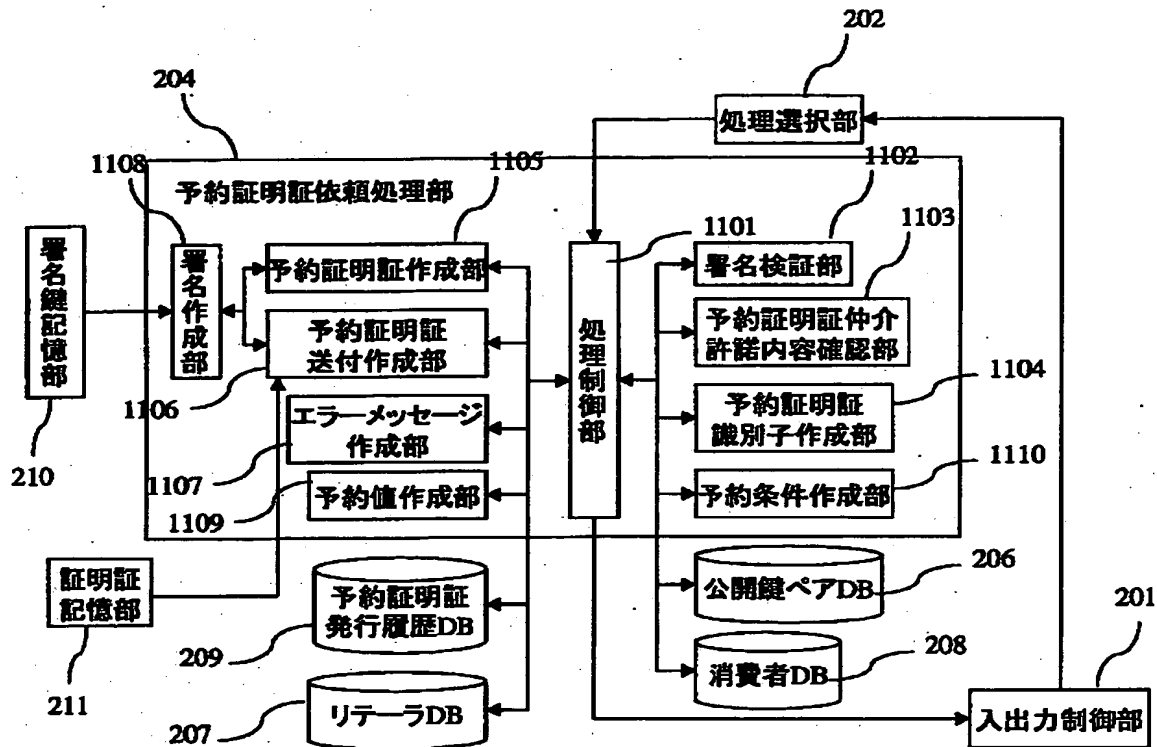
【図 9】

消費者識別子	消費者秘密情報
CNS10001	10110...
CNS10002	11000...
CNS10003	01110...
...	...

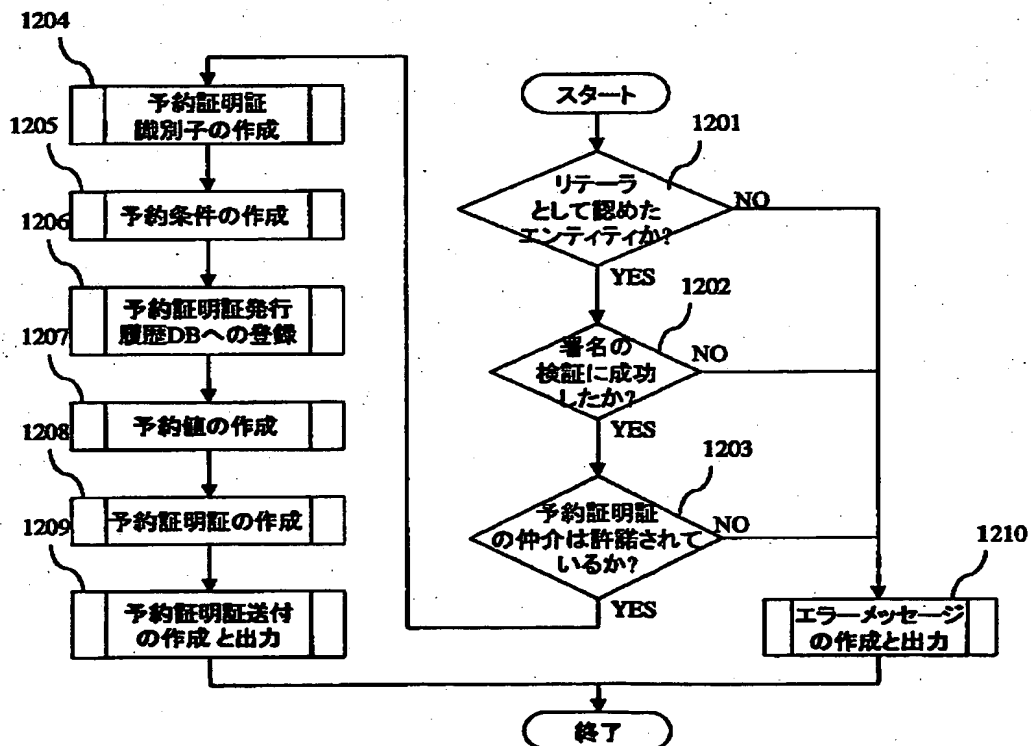
【図 1 0】

公開鍵識別子	プロバイダ識別子	消費者識別子	仲介者識別子	予約条件	発行日
PK00001	PRV10001	CNS10001	RTL10002	2F34A...	2000.2.1
PK00002	PRV10003	CNS10001	RTL10002	44FBC...	1999.4.16
PK00002	PRV10003	CNS10003	RTL10001	5AAB1...	1999.11.12
...

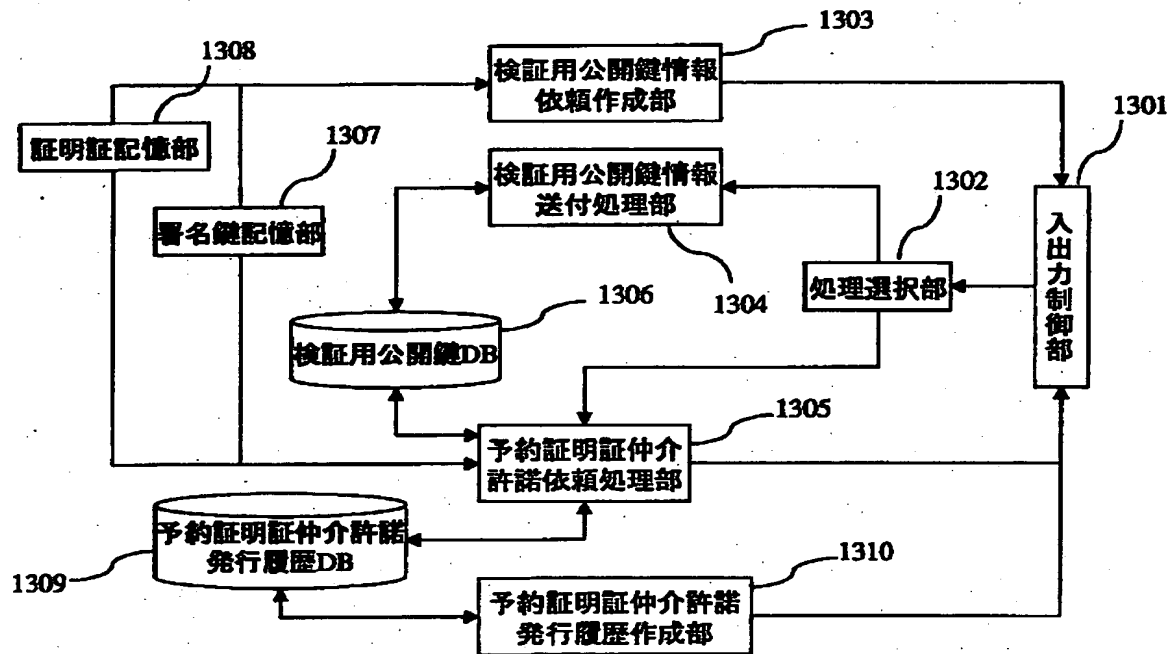
【図 1 1】



【図 1 2】



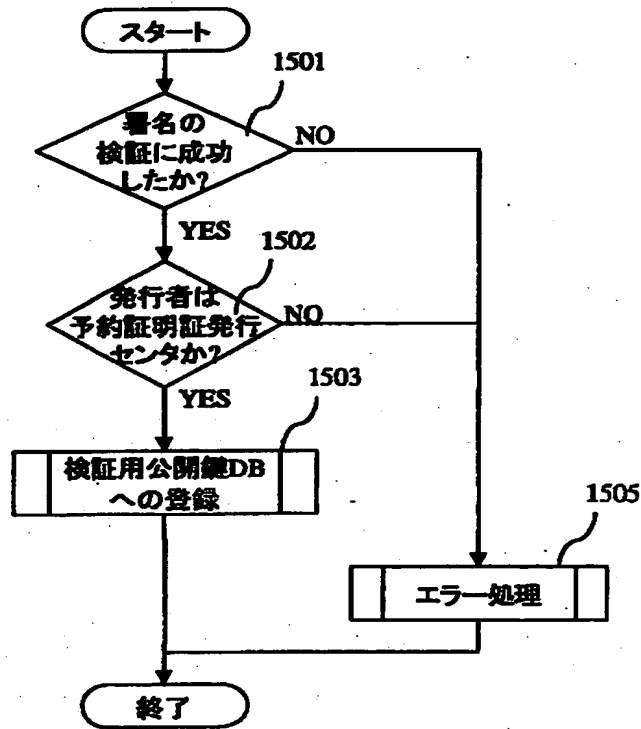
【図 1 3】



【図 1 4】

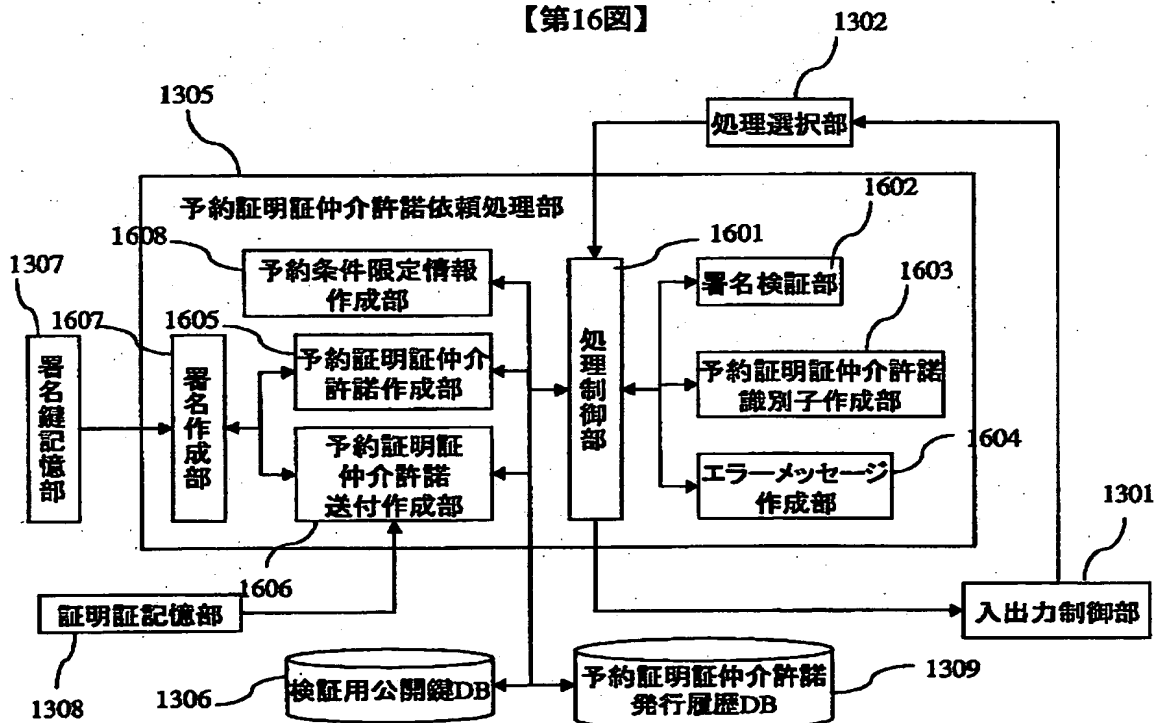
公開鍵識別子	法数	公開鍵	有効期間開始	有効期間終了	用途
PK00001	10110...	11001...	2000.1.1	2001.1.1	TT3 鑑賞券
PK00003	11111...	10000...	1999.11.1	2000.5.1	Millennium Watch Black
PK00007	11000...	10110...	1999.8.1	2000.2.1	GWJr コンサート 2000.1.15S 席
...

【図15】

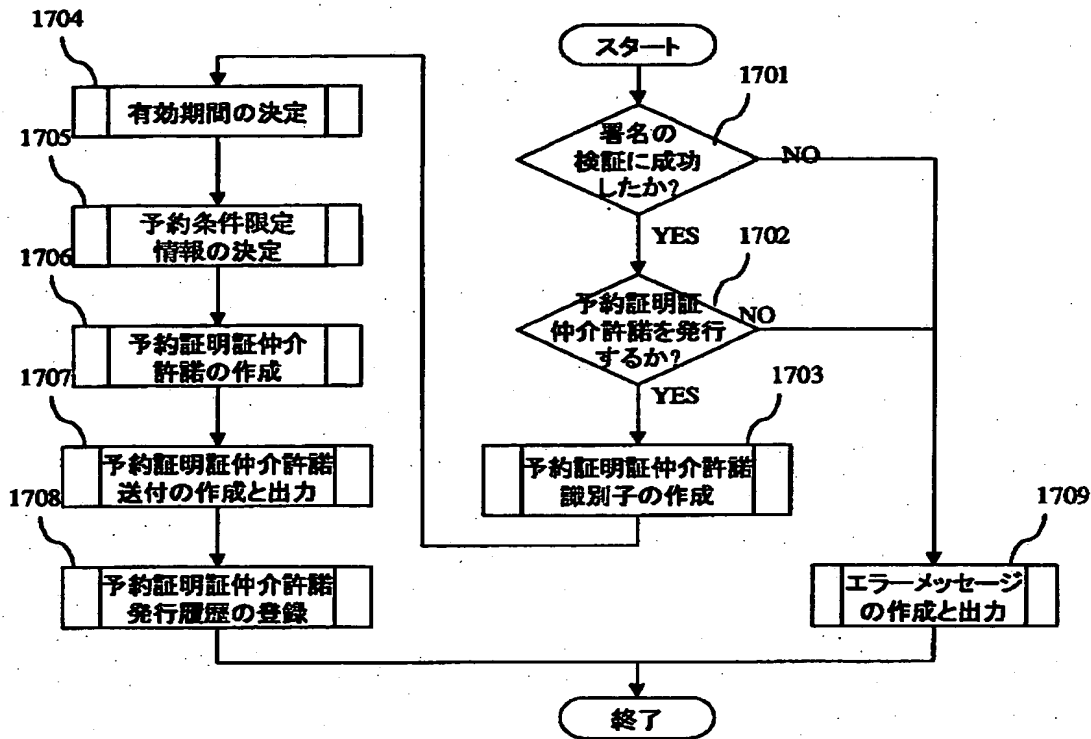


【図16】

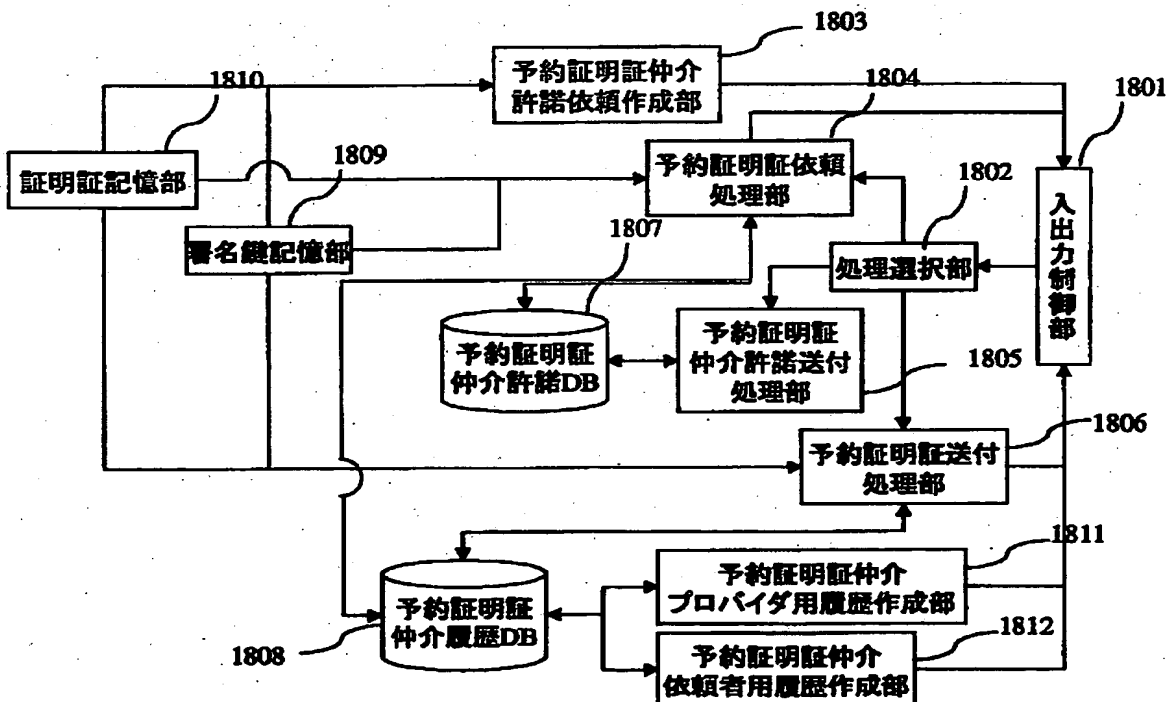
【第16図】



【図 17】



【図 18】



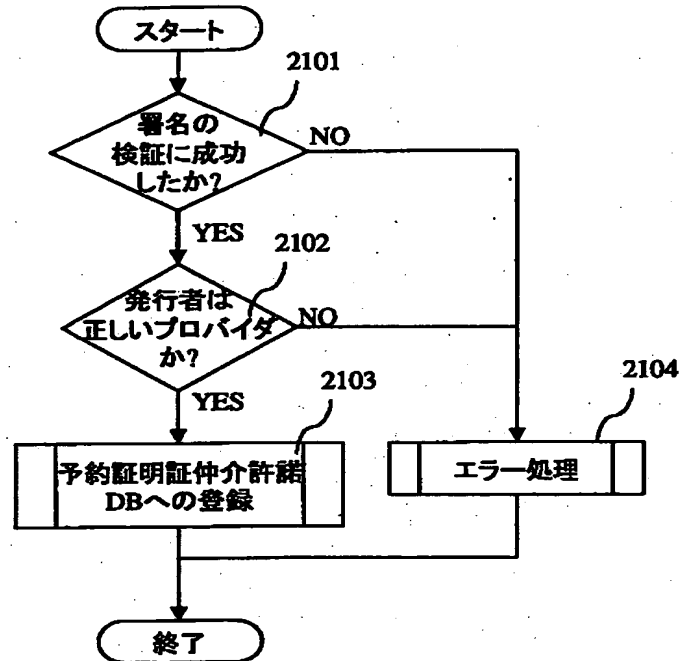
【図 19】

予約証明証仲介 許諾識別子	公開鍵識別子	プロバイダ識別子	予約証明証仲介許諾	プロバイダ証明証
AGM01002	PK00001	PRV10001	FF3AC4...	FE66B...
AGM03010	PK00002	PRV10003	FF3CC2...	FEE4A...
AGM03034	PK00008	PRV10003	FFF87A...	FE7DE...
...

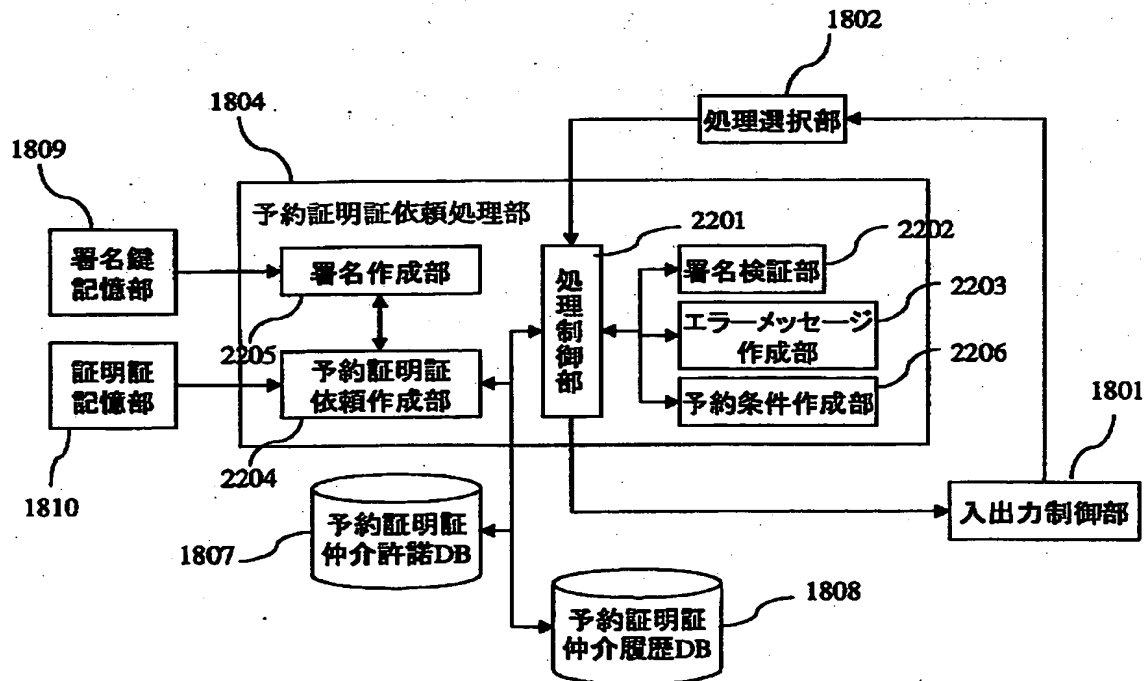
【図 20】

予約証明証 識別子	公開鍵 識別子	プロバイダ 識別子	消費者 識別子	依頼者 識別子	予約条件	依頼日時	発信日時
TKT10004	PK00001	PRV10001	CNS10006	CNS10006	2F34A...	2000.2.1 10:25	2000.2.1 10:27
TKT10010	PK00008	PRV10003	CNS10003	RTL10024	44FBC...	2000.2.16 18:03	2000.2.16 18:04
	PK00001	PRV10001	CNS10012	CNS10012	5AAB1...	2000.3.1 03:54	
...

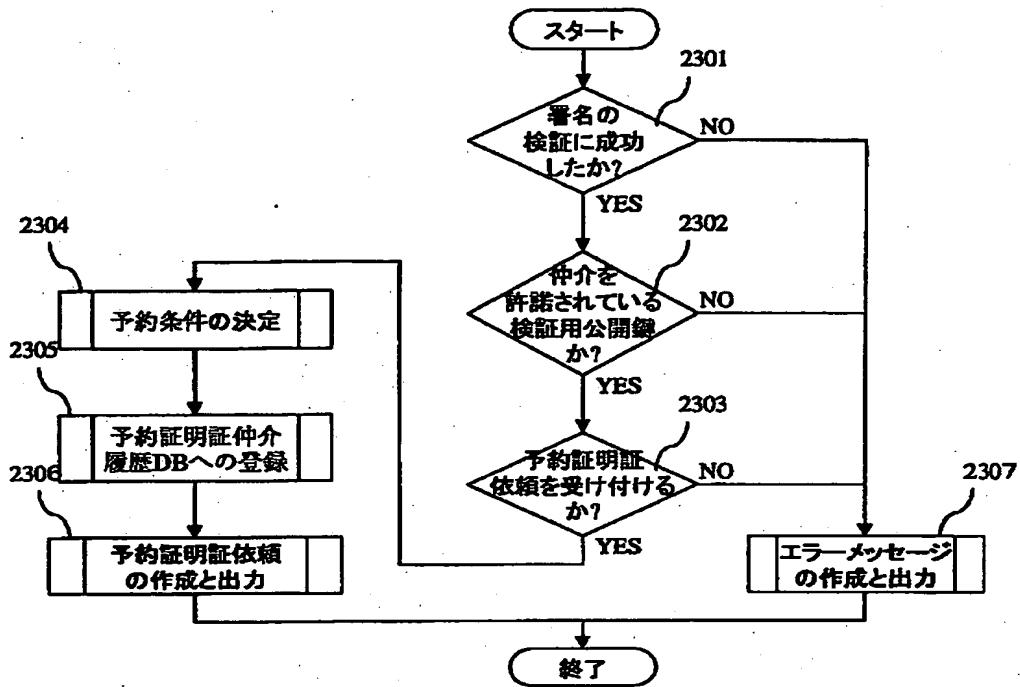
【図 2 1】



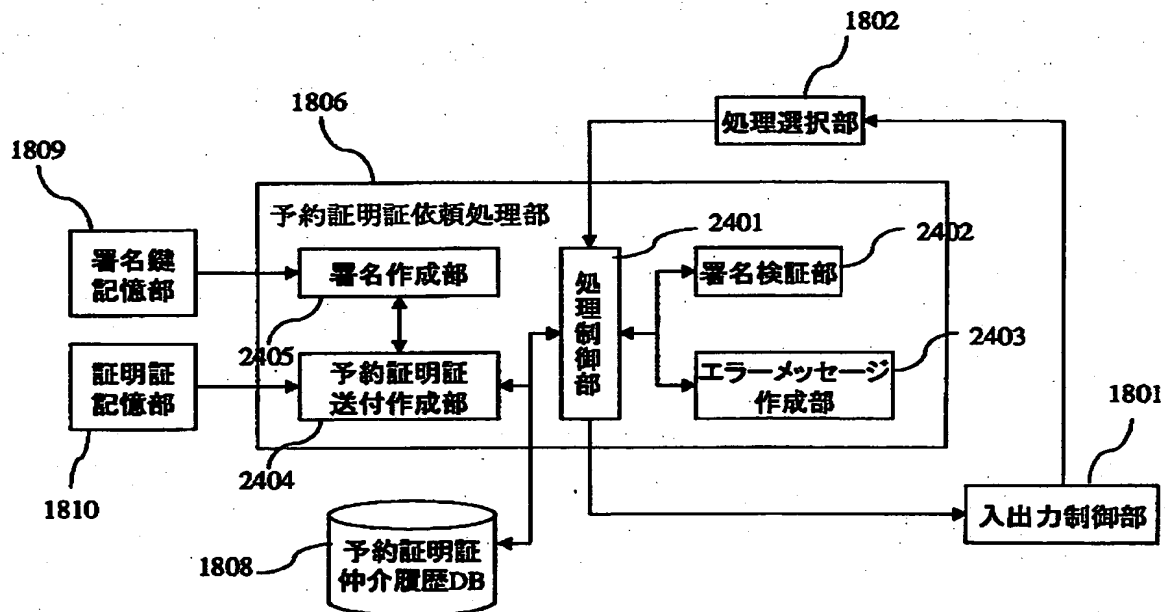
【図 2 2】



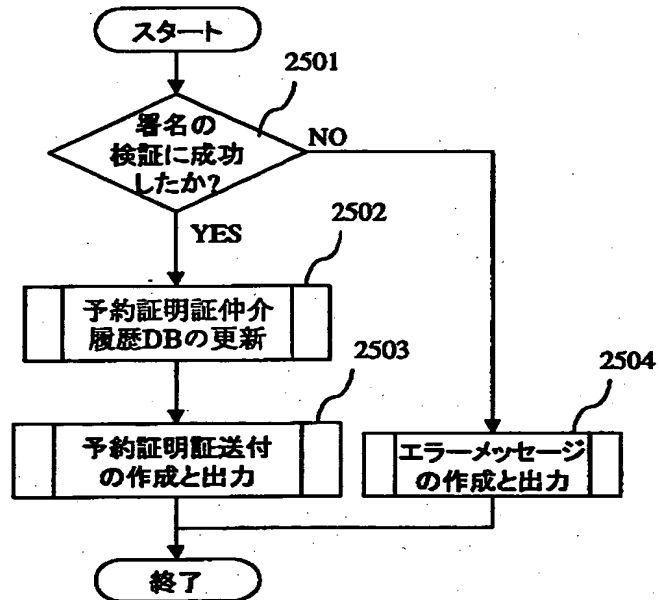
【図 2 3】



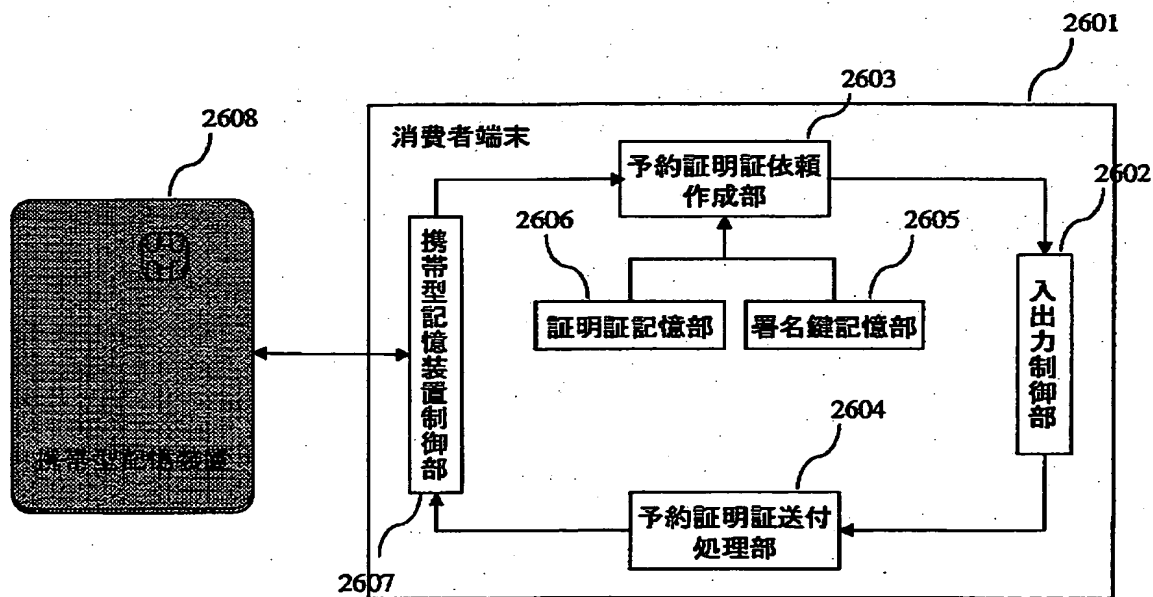
【図 2 4】



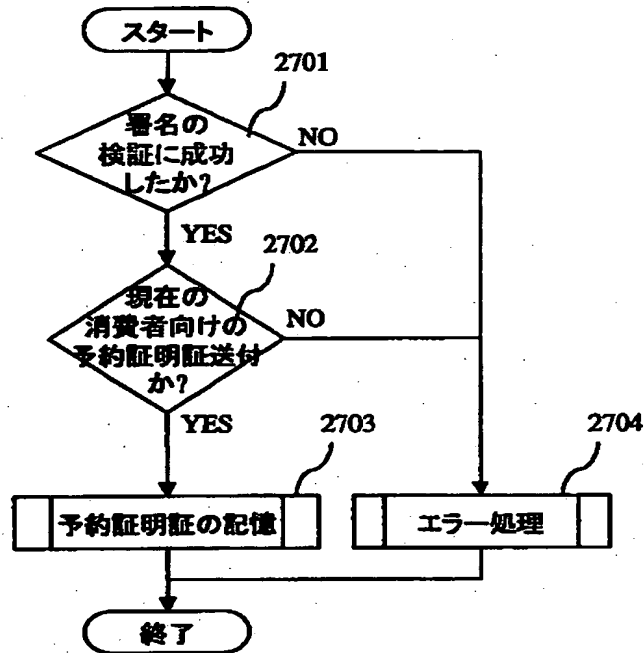
【図 2 5】



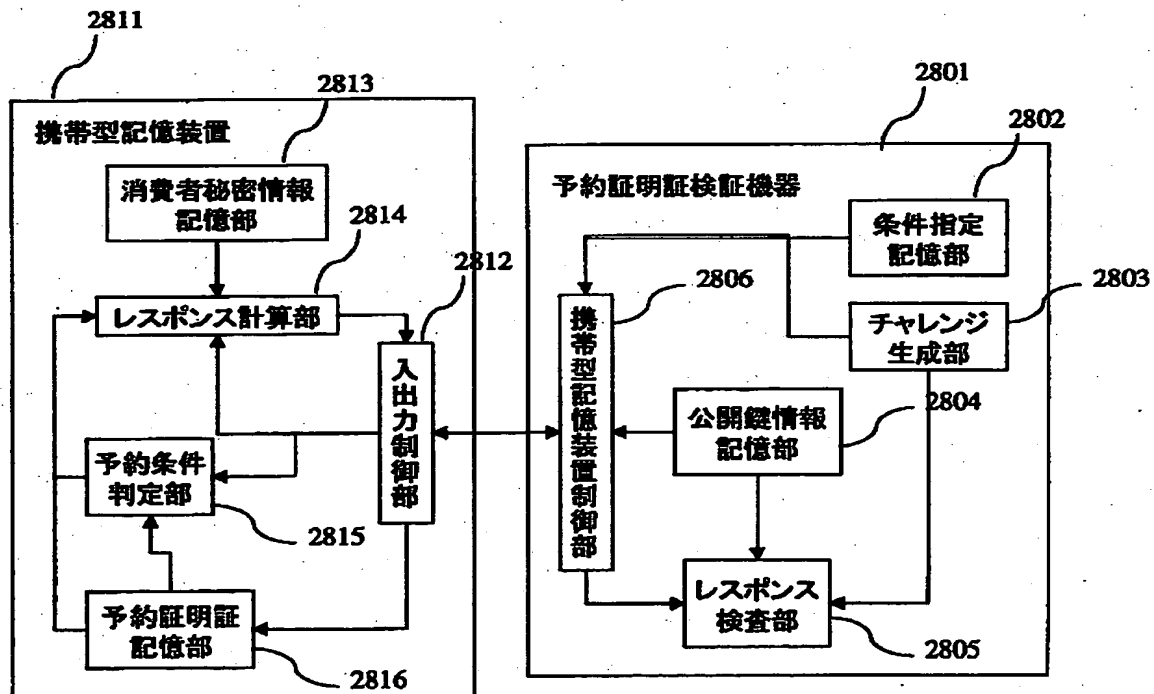
【図 2 6】



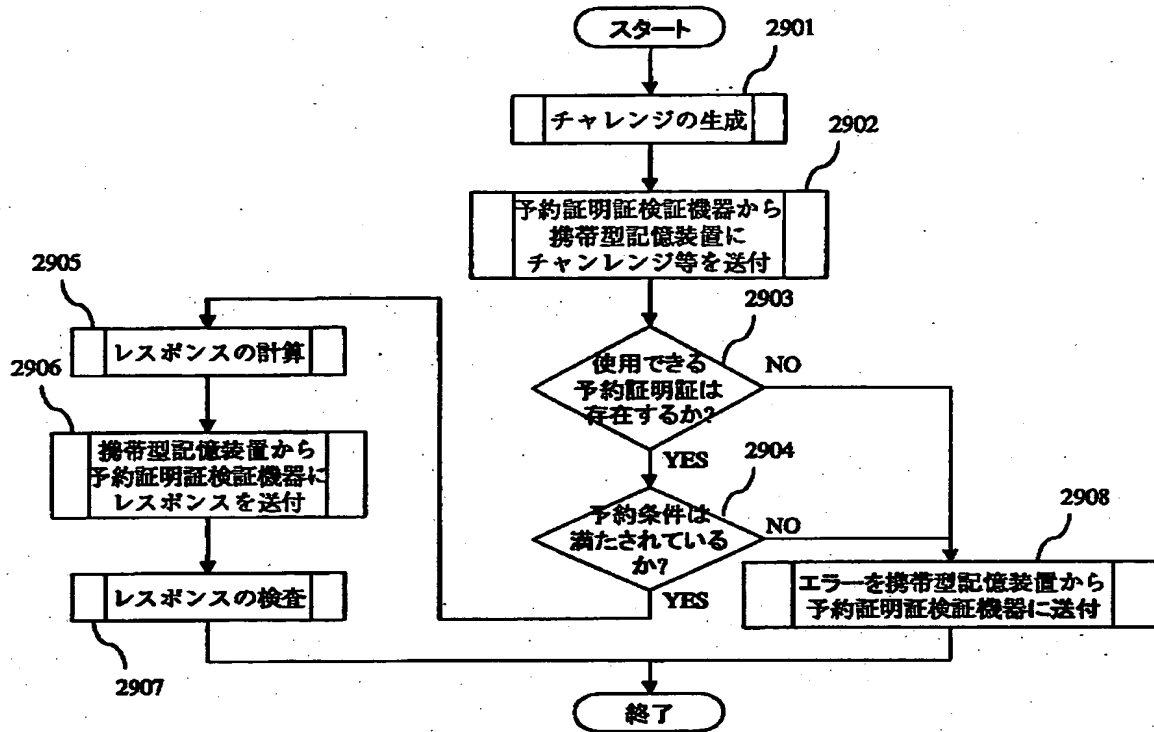
【図 27】



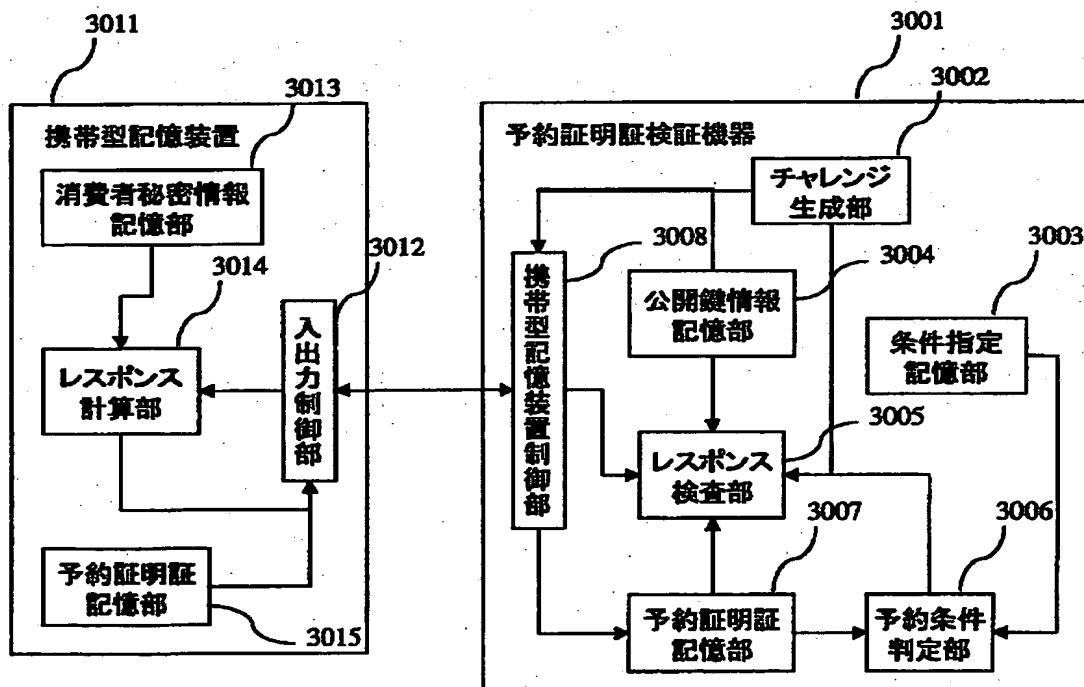
【図 28】



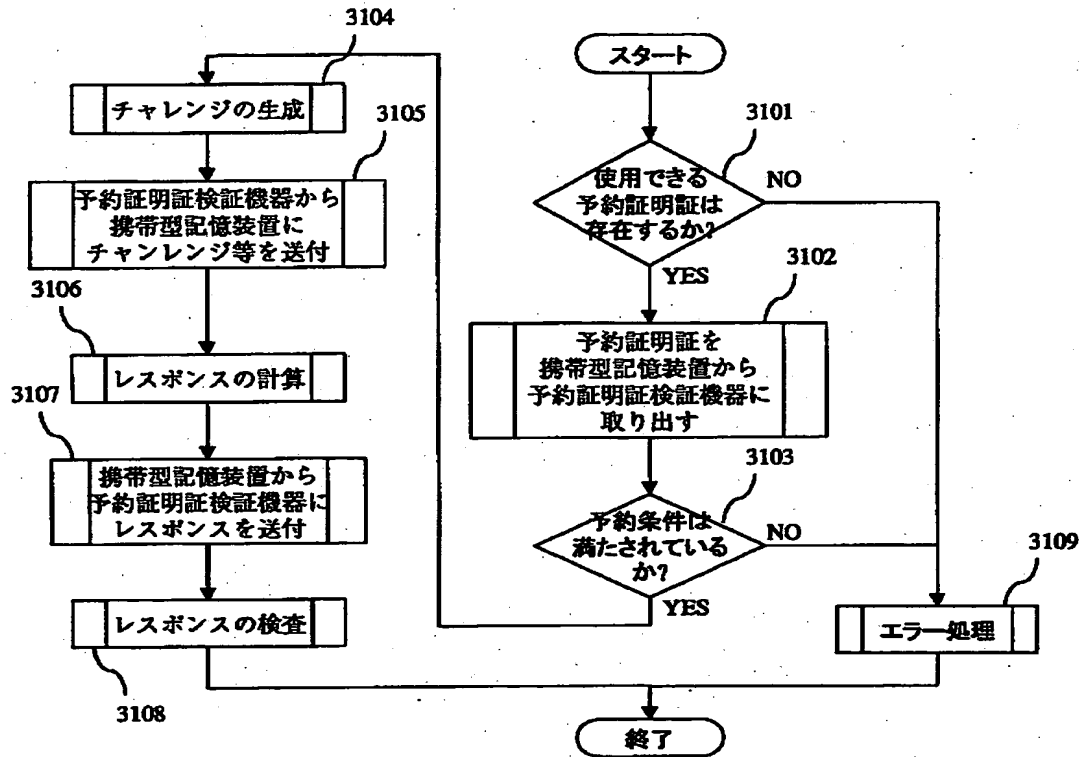
【図 29】



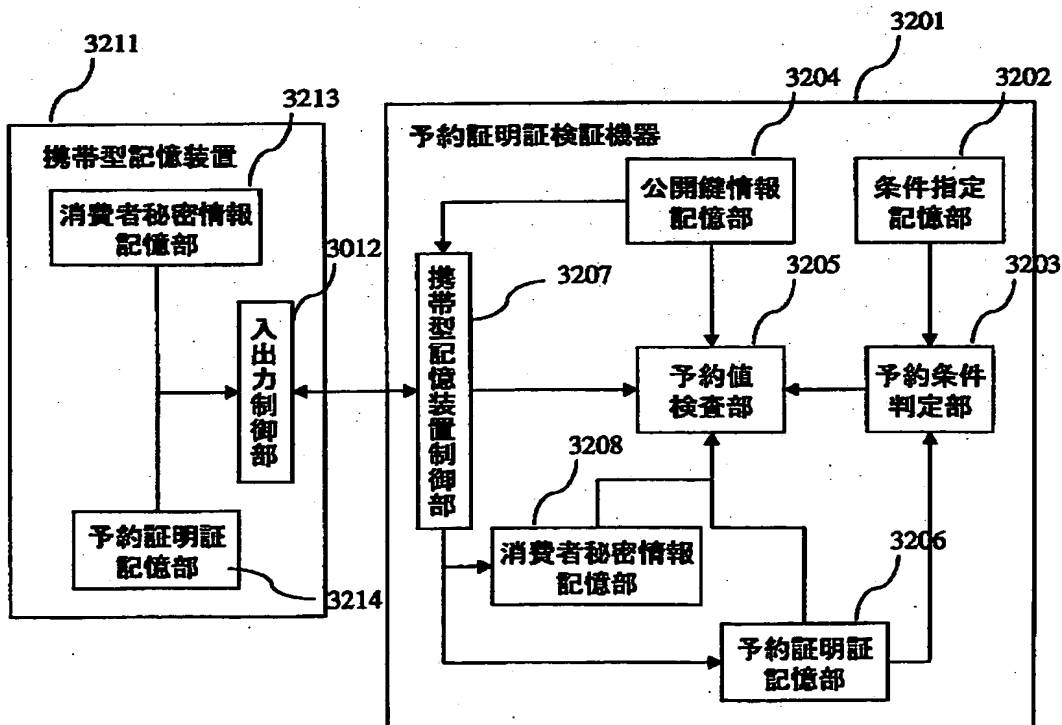
【図 30】



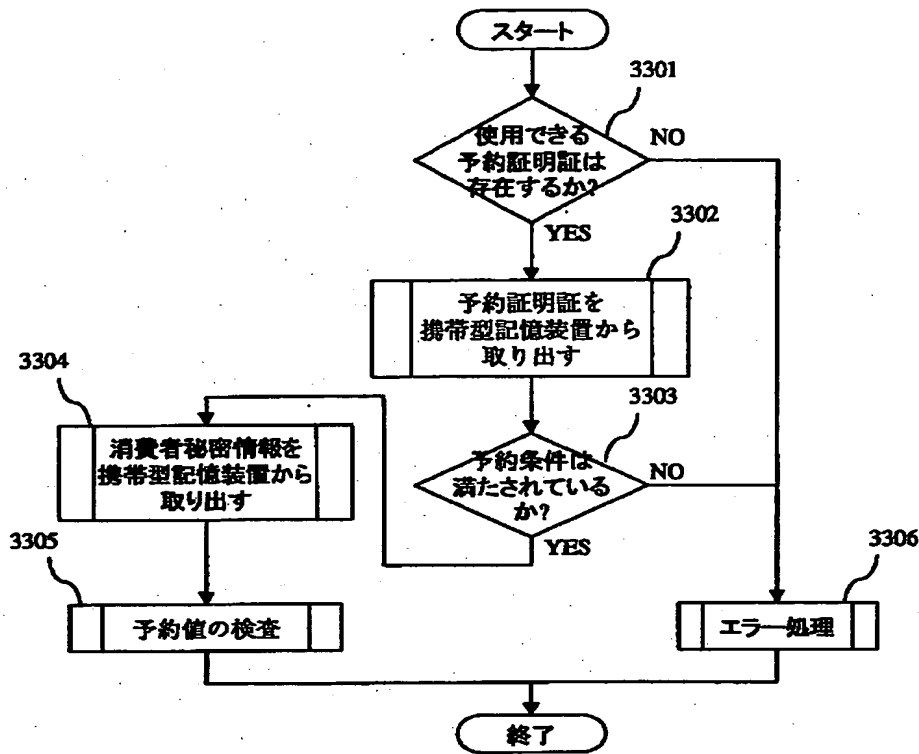
【図 3 1】



【図 3 2】



【図 3 3】



【図 3 4】

予約証明証仲介 許諾識別子	公開鍵 識別子	リテーラ 識別子	予約条件 限定情報	有効期間 開始	有効期間 終了	発行日
AGM01002	PK00001	RTL10001	FF3AC4...	1999.12.1	2000.11.31	1999.12.1
AGM03010	PK00002	RTL10003	FF3CC2...	2000.1.1	2000.7.1	2000.1.1
AGM03034	PK00008	RTL10003	FFF87A...	2000.3.4	2001.3.4	2000.3.3
...

【書類名】 要約書

【要約】

【課題】 予約販売業者が自らのリソースを消費することなく予約証明証を発行できるようにする。

【解決手段】 消費者端末109からインターネット101を介してリテーラ103に予約が行われる。リテーラ103は商品や予約者に応じた予約証明証の発行を予約証明証発行センタ102に要求して予約証明証を受領する。消費者端末109はリテーラ103からインターネット101を介して予約証明証を受け取り、これを用いて正規の予約者であることをプロバイダ105に関連する検証機器106で検証を受ける。予約者は、検証が成功したら商品やサービスの提供を受けることができる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005496]

1. 変更年月日 1996年 5月29日
[変更理由] 住所変更
住 所 東京都港区赤坂二丁目17番22号
氏 名 富士ゼロックス株式会社